Departamento de Matemáticas e Instituto de Ciencias Matemáticas

Universidad Autónoma de Madrid

Congruence problems and questions regarding sequences of numbers

Memoria de Tesis Doctoral presentada por

Ana Zumalacárregui Pérez

para optar al título de Doctor en Ciencias Matemáticas

Programa de Doctorado de Matemáticas

Trabajo supervisado por

Francisco Javier Cilleruelo Mateo,
Profesor Titular del Departamento de Matemáticas,
Universidad Autónoma de Madrid

Octubre de 2014

A mis padres.

Gracias

Para mí ha sido un placer poder invertir los pasados años en esta magnífica aventura. Me siento muy afortunada porque tengo la oportunidad de dar las gracias. A tanta gente que me ha ayudado en el camino y a tantos de los que he podido aprender tantas cosas. Gracias a todos, a los que sea capaz de nombrar y a los que por desgracia olvidaré.

En primer lugar, quisiera darle las gracias a Javier Cilleruelo, que no sólo me ha demostrado que es un gran matemático, un gran docente y una gran persona, sino que para mí ha sido un gran director de tesis. Estoy enormemente agradecida. Por haber sido tan generoso conmigo, compartiendo tus problemas e involucrándome en tantos proyectos interesantes, por haberme mostrado tantas matemáticas hermosas. Te estoy especialmente agradecida por haberme dado la confianza y libertad también para buscar mis propios proyectos. Gracias por apoyarme y por haberme dado siempre tu sincera opinión, que sabes que valoro mucho.

También tengo mucho que agradecer a Juanjo Rué. Hemos trabajado mucho juntos y he disfrutado mucho de la experiencia. Eres una de esas personas que hacen que sucedan cosas a su alrededor, he tenido mucha suerte de haber podido aprender tantas cosas de ti. Cuando te fuiste ya nunca fue lo mismo. Gracias por haberme regalado tu tiempo y tu sonrisa.

Durante estos cuatro años he tenido la gran suerte de poder viajar y trabajar con gente por todo el mundo. Quisiera agradecer a Moubariz Garaev por haberme acogido en Morelia dos semanas y por haber sido siempre tan amable y generoso conmigo. I would also like to thank Igor Shparlinski for giving me the opportunity to go to Australia and, specially, for giving me the opportunity to work with him. Thank you for hosting me these three months and helping me to feel like home. I was also very lucky to meet Pieter Moree and even luckier to get the chance to go to MPIM not once but twice to share my work and discuss about Mathematics and some other things with very interesting people; thank you Pieter for being such a great host. También quisiera aprovechar para agradecer a Harald Helfgott por haberme dejado participar de aquella estupenda escuela AGRA, aprendí mucho y sobre todo tuve la oportunidad de conocer a muchos matemáticos de América Latina. Se trata de una gran iniciativa, me encantará poder participar en Perú, gracias por contar conmigo.

Me siento muy afortunada porque, además de haberme podido mover por el mundo, también desde nuestra base en Madrid hemos recibido muchas visitas y eso me ha permitido conocer a muchos matemáticos. Thank you Endré Szemerédi for sharing with us a priceless month, so many discussions and stories. Thanks to Josef Solymosi, Suria Ramana, Olivier Ramaré and

Pedro Berrizbeitia for visiting us and sharing your time (and even sometimes your favourite problems) with me. También tuve la gran suerte de participar en la organización del primer Young Workshop in Arithmetics and Combinatorics, donde pude conocer a Julia Wolf, Tom Sanders, Pablo Candela, Giorgis Petridis, Dieter Mitsche, Arnau Padrol, Guillem Perarnau o Lluis Vena, entre otros; personas con las que he podido coincidir sucesivamente en congresos y que siempre han tenido un gesto amable y cariñoso para mí. Gracias Javier, Oriol y Marc hacerme partícipe de esto.

Quisiera también hacer un hueco especial a mis hermanos matemáticos. Rafa, ha sido un placer haberte conocido y haber disfrutado de tantos buenos momentos en la pizarra. Carlos, trabajar contigo ha sido una experiencia muy enriquecedora, me quedo con tu capacidad para compartir y gracias tambíen por compartir conmigo las mejores comidas y las mejores sobremesas. Serás un gran maestro. Thank you Paulius for so many fruitful discussions on the blackboard and for always pushing me a bit further.

Muchas gracias Fernando por haberte tomado el tiempo y el cuidado de leer esta tesis y de hacerme tantas sugerencias. Gracias también por ser siempre tan amable y paciente conmigo, y por enseñarme tantas cosas interesantes a lo largo de todos estos años.

Tienen también una parte importante de *culpa* todos esos maestros que me enseñaron tantas cosas cuando todavía no sabía qué persona quería ser: Miguel Ángel, Guillermo, Javier Holgado, María Pose o Leonor. Y también todos esos profesores con los que descubrí tantas cosas cuando aún no sabía qué clase de matemática quería ser: Antonio Córdoba, Juan Luis Vázquez, Andrei Jaikin, Enrique González o Dimitri Yakubovich, entre otros. Me habéis hecho enamorarme de las matemáticas una y otra vez. Siento que le debo una mención especial a Adolfo Quirós, que me ayudó a encontrar mi camino en un momento en el que estaba muy perdida. Gracias a todos.

Desde que empecé la tesis, sabía que mi paso por el Departamento sería temporal. Un tiempo prestado, casi robado. Sin embargo esto no impidió que se convirtiera en mi segunda casa. Eso sin duda no podría haber pasado sin una legiíon de becarios y gente joven que, como siempre dice Carmen, es lo mejor que tiene este departamento. Gracias a todos por vuestros grandes momentos, por los cafés, los friki viernes, las comidas y discusiones eternas sobre política, gracias por venir a los seminarios junior y gracias por dejarme siempre preguntar, gracias por dejarme jugar al fútbol, por dejarme ganar al voley playa y por organizar tantos planes juntos. A los que se fueron: Angélica, Moisés, Pedro, Razvan o Charro, lo dejasteis todo muy bien montado. Gracias. A los nuevos que llegaron: Leyter, Adri, Marcos, Juan, Irina, María o Iason, antes de que os déis cuenta seréis los mayores, preparaos. A los que siempre estuvieron allí: Alberto, Mari Luz, Elena Sofía, Carlos Abad, Bego, Dulci, Belén y Diana. Y a los que espero que siempre estén ahí: David Torres, Jose y Beatriz, os espero en Australia. Gracias a todos, por tantos buenos momentos. También a todas esas personas que, aunque ya no son necesariamente becarios, hacen del Departamento un sitio del que no querer marcharse (ojalá no tengan nunca que marcharse): Ana Primo, Adrián Ubis, Mari Jose. Gracias a Antonio, Paloma y Cristina, gracias a Carmen y Ana Bravo, a Eugenio Hernández, a Fernando Quirós, a Jose Luis Torrea y a Mavi Melián.

Ha sido una suerte para mí poder contar con una segunda segunda casa: el ICMAT. Gracias también a toda la gente con la que he compartido el tiempo allá: Joan, Javi, Ángel o Carlos Pastor, Giancarlo, David Fernández y Víctor García, por buenos ratos y comidas juntos. Gracias Ágata por liarme tantas veces y llevarme a hacer tantas cosas interesantes. Gracias a David Martín de Diego por organizar tantos saraos de divulgación. Gracias Leo por el Seminario Junior y por lo todo lo demás. Gracias a Eduardo Frechilla, a Arucas, a Esther Fuentes y a Manolo, por haberme permitido organizar tantas cosas para llenar de vida el instituto.

Gracias, Pablo. Por haberme enseñado lo que significa ser matemático y por haber compartido tantas cosas hermosas conmigo. Crecimos juntos por el camino y eso lo guardaré siempre.

Hay dos compañeros de viaje sin los que no sé muy bien a dónde hubiera llegado: Félix y Sera (si no fuera por Sera, no sé qué hubiese sido de mí estas últimas semanas de trámites: eres muy grande). Los tres hemos trabajado muy duro estos años y hemos compartido un máster juntos, que no es poco. Hemos compartido un 613 y mucha comida china. Gracias por haberme regalado tantos buenos recuerdos y por las sesiones de terapia doctoral, que creo que son las que nos han permitido mantenernos cuerdos todo este tiempo. El viaje continúa. Os quiero mucho, chicos.

Guardo un huequito especial para todas esas personas que me han aguantado todo este tiempo, aunque no siempre me dejen hablar de mates. Mis chicas: Tamara y Esther, vivir con vosotras me ha traído grandísimos momentos, es una etapa que no olvidaré. Gracias a Marta y Olvido, mi familia, y que me conocen mejor que yo misma. Gracias a Bolo y a Víctor por sacar adelante la Malapata, que tantos buenos ratos me ha traído, y por hacerme creer que era la capitana. Gracias a los físicos: Javi (aunque no sea físico), Iván, David o Laisfer, por incluirme en vuestros planes y vuestros chori breaks. Gracias a los otros físicos: Ana, Gonzalo, Emilio o Brian, por las paridities y por los cafés. Gracias a Pabo, David, Africa, Saray, a Ana y Mauro. Gracias por volver a llevarme al mundo real de vez en cuando.

Los que me conocen bien saben que no se puede entender quién soy sin conocer a mi familia. A mis primos y tíos, a los que quiero con locura, y que me hacen sentir como en casa aunque esté a miles de km. Gracias. Gracias a Teo y Rosi, mis tías favoritas, por hacerme comida rica de vez en cuando y haber sido siempre tan buenas conmigo. A mi hermano, mi único hermano que siempre fue y será un ejemplo a seguir para mí. Fue estupendo poder compartir tantas charlas nocturnas sobre ciencia cuando vivíamos juntos y fue genial compartir una infancia tan divertida. Gracias, Miguel. A mis padres les estaré siempre agradecida, no por esta tesis, pero porque me han enseñado todo lo importante, a ser generosa y compartir, a ser agradecida y cuidadosa, y porque gracias a ellos he podido ser quien yo quería ser. Gracias por vuestro apoyo, incluso cuando elijo marcharme tan lejos. Gracias por haberme ayudado crecer y querer ser mejor. Gracias por darme la vida.

Gracias, Luis Daniel. Gracias por quererme como soy y gracias también por seguirme hasta el fin del mundo. Gracias por hacerme tan feliz.

Contents

Prologue

During the past years I had the chance to work on many different problems, some of them can be found in this manuscript. I deeply enjoyed the time spent obtaining these results and learning about the problems and techniques that will be discussed here. However, I must admit that it has been hard for me to complete the writing of this thesis. Harder than I thought. I did not seem to find the right closure to this journey. I simply could not choose the right words. And yet.

I believe that my broad mathematical interests and curiosity are reflected on this manuscript, which might look like an unstructured set or collection of problems, each of them seem to require of different techniques and intuition, but in fact it contains many common points and perspectives. In the end, working on those problems shaped my mathematical taste along the way. All over these years I worked on several questions in number theory with a combinatorial flavour and this thesis could be considered to live in the interface of the Analytic Number Theory, Elementary Number Theory and the so called Additive Combinatorics.

The presented manuscript is divided into two different parts: congruence problems and questions regarding sequences of numbers. Here I will briefly discuss what kind of problems and techniques will appear in the following chapters, without discussing in detail the background or state of the art of every problem, which has been carefully introduced at the beginning of each chapter.

Most of the given results, specially those in Chapter 2, rely or depend on various complementary results, sometimes classic and sometimes new, which have been included in Appendix A at the end of the manuscript.

◂ Congruence problems ▸

A large component of my work relies on the study of the solutions to congruence problems. The question is, essentially, to obtain non-trivial estimates for

$$|\{\mathbf{x} = (x_1, \dots, x_k) : f(x) \equiv 0 \pmod{p}\} \cap B|, \tag{1}$$

where f is a nice function (polynomial, exponential, etc) and B is usually the direct product of intervals (a box) lying in the abelian group where the solutions $\mathbf{x}$ live.

These type of problems have been intensively studied and gave arise to very interesting mathematics along the way. Think for example in points on a variety

$$V: \quad f_j(x_1,\dots,x_n) \equiv 0 \pmod{p}, \quad j=1,\dots,m.$$

One would like the points in V to be harmoniously distributed in the hypercube $[1,p]^n$, but for a given box B does the number of points $|V \cap B|$ agree with the value predicted by heuristic arguments? In other words: can we assure that

$$|V \cap B| = \frac{|B|}{p^n}|V|(1+o(1))?$$

It is clear that when the size of the box is too small one cannot expect to have any kind of asymptotic result, since the expected number of points could be less than one. Even when the box is substantially bigger, one does not have in general an asymptotic of this kind due to geometrical restrictions (see [44] for a more general discussion and examples). Nevertheless, in many interesting situations one can prove the equidistribution for the quantity in (1). See for example [45, 73, 97].

Such distribution results naturally depend on classical exponential sums techniques, which in most cases rely on deep results in Algebraic Geometry -related to the so called Riemann Hypothesis for curves or varieties- but sometimes can be directly deduced from certain additive properties of the sets in question. In fact, for any given set A in order to derive good estimates for the distribution of points in A it suffices to show that -for at least a large number of non-trivial characters ψ- we have

$$\left|\sum_{a\in A}\psi(a)\right| \ll |A|^{1/2}. \tag{2}$$

It is easy to check that for any set A in an Abelian group

$$|A|^{1/2} \ll \max_{\psi\neq\psi_0}\left|\sum_{a\in A}\psi(a)\right| \leq |A|.$$

This means that the bound in (2) is essentially best possible. Many of the geometrical obstructions we can find in this problem can be translated into this language: the desired set must be *well distributed along characters*. We dedicate Section 1.2 to find many examples of sets satisfying this property.

Estimates for the quantity in (1) are non-trivial up to a certain threshold on the size of B which, due to the classical exponential sums techiques, includes some logarithmic factor. Chapter 1 includes the results in [32], which improve the error term on these estimates for a general class of congruence problems, extending the range for an asymptotic formula as a result. The proofs are based on ideas of Garaev [46] and Cilleruelo [21]. The results are stated in a very general way and the proofs combine both combinatorial arguments and exponential sums techniques.

The study of this problem in such a general way provides a good approach to a different type of question. In Section 1.3 we use similar arguments to deal with an additive problem in

finite fields with powers of elements of large multiplicative order. For a given finite field $\mathbb{F}_q$, we study sufficient conditions which guarantee that the set $\{\theta_1^x + \theta_2^y : \ 1 \le x \le M_1, \ 1 \le y \le M_2\}$ represents all the non-zero elements of $\mathbb{F}_q$. We investigate the same problem for $\theta_1^x - \theta_2^y$ and, as a consequence, we prove that any element in the finite field of q elements has a representation of the form $\theta^x - \theta^y, \ 1 \le x, y \le \sqrt{2}q^{3/4}$ whenever θ has multiplicative order at least $\sqrt{2}q^{3/4}$. This improves the previous known bound for a question posed by A. Odlyzko. The proof again combines classical arguments on exponential sums with additive combinatorial arguments based on the structure of certain Sidon sets and is included in [31].

In Chapter 2 we focus on the problem of estimating the quantity in (1) when the box B is qualitatively smaller. As we said before, beyond certain threshold no asymptotic formula is possible. In particular, for such a small box one can only study the concentration of solutions and derive upper bounds on the number of points on curves that hit in. This question was introduced by Cilleruelo and Garaev [22] for the special case of a modular hyperbola and later in [23] a series of general results were obtained in this direction. In this case, classical exponential sums techniques do not apply and one must exploit additive combinatorial arguments to improve the trivial bound in this range.

In Section 2.1 we present upper bounds for the number of solutions

$$Q(x, y) \equiv 0 \pmod{p}, \quad (x, y) \in B,$$

where $Q \in \mathbb{Z}[X, Y]$ is an absolutely irreducible (modulo p) quadratic polynomial of non-zero discriminant. This result, which generalizes the main result in [22], was included in [103] and it is presented here as a warm up for the sections to come in Chapter 2.

The rest of the chapter contains a combination of the results obtained in [16] and [28]. In particular, this problem is studied for a general class of curves

$$(x, y): \quad f(x) \equiv y \pmod{p} \quad \text{or} \quad f(x) \equiv y^2 \pmod{p}, \quad f \in \mathbb{Z}[x].$$

In many cases we obtain non-trivial estimates and also improve some of the previous known bounds. In some parameter ranges, when the box is very small, our results are the best possible and could be considered as modulo p analogues of the results of Bombieri and Pila [8] on the number of integral points on plane polynomial curves.

The proofs in Sections 2.2-2.4 rely on serious connections between the problem of distribution of points in small boxes on modular curves with some delicate combinations of results from Geometry of Numbers, Diophantine approximation theory, the Vinogradov mean value theorem and the Weyl method.

The results described here are not only deep, interesting and surprisingly general, but also have attractive applications. These are contained in Section 2.4 and go from the study of isomorphism classes of hyperelliptic curves in some thin families to the diameter of partial trajectories of a polynomial dynamical system modulo p.

Unfortunately, our results do not cover all ranges of B. Additive Combinatorics approach seem to be very fruitful for very small boxes and classic exponential sums are efficient up to a

certain threshold as well. Let us think, for example, on the points of an elliptic curve

$$E_{a,b}: \quad y^2 \equiv x^2 + ax + b \pmod{p}.$$

When we consider the number of points in a square $(x, y) \in B$, we have:

▸ Asymptotic results: $|E_{a,b} \cap B| \sim |B|/p$ if $|B| = \omega(p^{3/2})$.

Due to algebraic geometry methods and classical exponential sums techniques, which can be pushed a bit further and give non-trivial bounds up to $|B| \gg p$.

▸ Optimal upper bounds: $|E_{a,b} \cap B| \ll |B|^{1/6+o(1)}$ if $|B| \leq p^{2/9}$.

Obtained via additive combinatorial methods. In fact, with the different approaches described in Section 2.2.1, we are able to obtain non-trivial bounds for this quantity (that is $o(|B|^{1/2})$) up to $|B| = o\left(p^{2/3}\right)$.

This means that, in the range $p^{2/3-\epsilon} \leq |B| \ll p$ our methods are not strong enough. Very recently, Chang [15] obtained non trivial upper bounds of the type $|B|^{1/2-\epsilon}$ for this quantity in the wider range: $p^{\epsilon} \leq |B| \leq p^{18/23}$, but there is still a gap for which nothing is known. It seems that neither classical exponential sum techniques nor the additive combinatorial ones are efficient in this range. It will be very interesting to find a method or develop techniques to deal with this intermediate range.

Observe that these problems can be generalized to finite fields. If instead of considering curves or values of polynomials on prime fields one moves the problem to generic finite fields $\mathbb{F}_q$ then the natural generalization of an interval should be an affine space. This question has been recently studied in several works such as [27, 86, 83].

▸ Sequences of numbers ◂

The rest of the work I present here has a common protagonist: sequences of natural numbers. In fact, not all the problems I will discuss here apply to sequences but to finite sets of numbers, but the results will hold asymptotically in the number of elements of the set.

▸ The least common multiple of a sequence:

In Chapter 3 we study the growth of the least common multiple of certain sequences. In particular, we study the asymptotic behaviour of the following function

$$\psi(S) = \log \operatorname{lcm}\{a : a \in S\},$$

on different families of sets S. This function is a natural generalization of Chebyshev's function $\psi(n)$, whose understanding was a key ingredient in the proof of the Prime Number Theorem. This chapter presents two complete different approaches to understand the function ψ, which somehow encapsulates -at least quantitatively- the arithmetic information of a set S of positive integers.

In Section 3.1 we study the logarithm of the least common multiple of the sequence of integers given by $1^2 + 1, 2^2 + 1, \ldots, n^2 + 1$. Using a result of K. Homma on the distribution of roots of quadratic polynomials modulo primes, we calculate the error term for the asymptotic

obtained by Cilleruelo [20]. The proofs exploit classical analytic number theory arguments and made a detailed study of the method introduced by Cilleruelo for general quadratic sequences. The results of this section can be found in [99].

In Section 3.2 we study the quantity $\psi(S)$ for a randomly chosen subset of $S \subseteq [n]$ considering two different models which are related to the $G(n,p)$ and $G(n,M)$ models for random graphs.

In the first, each element is chosen to belong to S independently at random with a certain probability $\delta = \delta(n)$. In the second model, one restricts attention to k-subsets of $\{1,2,...,n\}$ (where $k = k(n)$), picking among the $\binom{n}{k}$ possibilities uniformly and at random. In both cases, we obtain an asymptotic for the $\log(\mathrm{lcm}[S])$ that holds almost surely as $n \to \infty$. For example, we show that for almost all sets $A \subseteq \{1,\dots,n\}$: $\mathrm{lcm}\{a : a \in S\} = 2^{n(1+o(1))}$.

We compare the obtained results with previous results of Cilleruelo [20] on the lcm of values of a polynomial sequence and, in particular, to the polynomial studied in Section 3.1. For example, the leading term in Cilleruelo's asymptotic formula for

$$\log \mathrm{lcm}\left\{k^2+1 : k \le \sqrt{n}\right\} = \frac{1}{2}\sqrt{n}\log n + c\sqrt{n} + o\left(\sqrt{n}\right)$$

agrees with the almost-sure result for $\log \mathrm{lcm}[S]$ where S is a uniformly randomly chosen subset of $\{1,2,...,n\}$ of size $[\sqrt{n}]$, but that there is a difference seen in the secondary term.

This section contains the results from and [30], whose proofs involve elementary probability theory and prime number theory.

▸ Non-zero digits of combinatorial sequences:

Let $b \ge 2$ be a positive integer and S be an infinite sequence of integers. If the sequence have some combinatorial meaning, it is natural to think about how the representations of this elements in base b might look like. In Chapter 4 we study the following problem: for a sequence S with a given growth, how often elements in S can be written in base b with a small number of digits? This question has been studied before for well known combinatorial sequences such as $n!$ [69], Fibonacci numbers [93] or Catalan numbers [72], for example.

In this case, we follow a very general approach to show for a wide variety of sequences $\{a_n\}_{n=1}^{\infty}$ that for almost all n the sum of digits of a_n in base b is at least $c_b \log n$, where c_b is a constant depending on b and the sequence. Our approach covers several integer sequences arising from number theory and combinatorics and only depends on the growth of the sequence, not on arithmetical constraints.

In fact, we show that the previous statement holds for every sequence $\{a_n\}_{n=1}^{\infty}$, with

$$a_n = e^{f(n)}\left(1 + O\left(n^{-\alpha}\right)\right), \ \alpha > 0 \tag{3}$$

where f is a two times differentiable function satisfying $f''(x) \asymp 1/x$ for large x. The number of permutations, involutions, Cayley trees or Graphs on surfaces, among others, satisfy this growth condition.

We dedicate Section 4.1, to show that the sequence of Bell numbers satisfy the required growth condition (3). In this case, the analysis is more intricate since estimates for the size of the n-th Bell number depend on an implicitly defined function of n.

The results included in this chapter have been published in [25].

- g-Bases for intervals of integers:

There are many classical problems related to different restrictions on the representation function

$$r_A(x) = |\{(a, a') \in A \times A : \ a + a' = x\}|,$$

for sets or sequences A.

Good examples are Sidon sets, $r_A(x) \leq 2$, or additive basis, $r_A(x) \geq 1$, which can be studied in different contexts (finite groups, infinite groups, semigroups, intervals, etc.) giving arise to complete different questions.

In Chapter 5 we study the smallest cardinality of a g-Basis for intervals, that is $r_A(x) \geq g$ for every $x \in \{1, \dots, n\}$. Let

$$\gamma_g(n) = \min_{A \subset \mathbb{Z}} \{|A| : \ A \text{ is a } g - \text{basis for } \{1, \dots, n\}\}.$$

It is clear that such a minimum exist and it is easy to see that the quantity $\gamma_g(n)$ is of order $\sqrt{gn}$.

We study the quantities

$$\underline{\gamma_g} = \liminf_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}} \quad \text{and} \quad \overline{\gamma_g} = \limsup_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}}$$

and show that their limits in g coincide. In fact, we show that the value of such limit depends on finitely supported positive functions with small integral and large auto convolution on a fixed interval. The strategy follows the lines of [26], where the case of g-Sidon sets for intervals was studied (that is $r_A(x) \leq g$), and approaches the problem by considering successive constructions of sets whose support is restricted.

In order to do so, we exploit good constructions -based on ideas in [88]- of sets on finite groups whose representation function is *closed* to be constant. These constructions are included in Section 5.1, as well as some considerations regarding sets in finite groups with restricted representation function.

Following the ideas of Cilleruelo, Ruzsa and Vinuesa [26], we relate these g-basis discrete constructions with finitely supported positive functions having small integral and whose auto convolution is bounded from above on a fixed interval. In Section 5.2 we show how to connect the problem of constructing a function with certain autoconvolution properties from a set with the analogous properties on its representation function. Finally, in Section 5.3 we use the constructions for cyclic groups given in Section 5.1 to obtain a set whose representation function replicates the autoconvolution properties of a given function.

The results included in this thesis are contained in the following published research articles and preprints:

[16] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, Points on curves in small boxes and applications, *Michigan Math. J.*, 63(3):505–534, 2014.

[25] J. Cilleruelo, F. Luca, J. Rué and A. Zumalacárregui, On the sum of digits of some sequences of integers, *Cent. Eur. J. of Math.* 11(1): 188–195, 2013.

[28] J. Cilleruelo, I. E. Shparlinski y A. Zumalacárregui, Isomorphism classes of elliptic curves over a finite field in some thin families, *Math. Res. Lett.*, 19(2):335–343, 2012.

[30] J. Cilleruelo, P. Šarka, J. Rué, and A. Zumalacárregui, The least common multiple of sets of positive integers, *J. Number Theory* 144:92–104, 2014.

[29] J. Cilleruelo, C. Vinuesa and A. Zumalacárregui, Representation functions in finite groups and bases for intervals, *preprint*, 2014.

[31] J. Cilleruelo and A. Zumalacárregui, An additive problem in finite fields with powers of elements of large multiplicative order, *Rev. Mat. Complut.*, 27(2):501–508, 2014.

[32] J. Cilleruelo and A. Zumalacárregui, Saving the logarithm factor in the error term estimates of some congruence problems, *preprint*, 2014.

[99] J. Rué, P. Šarka and A. Zumalacárregui, On the error term of the logarithm of the lcm of a quadratic sequence, *J. de Théor. Nombres Bordeaux* 25(2):457–470, 2013.

[103] A. Zumalacárregui, Concentration points on modular quadratic forms, *Int. J. of Number Theory*, 7(7): 1835–1839, 2011.

Resumen y conclusiones

La tesis presentada contienen una serie de problemas que se podrían situar en la interfaz de la Teoría Analítica de números, la Teoría Elemental de números o la llamada Combinatoria Aditiva. El manuscrito se dividide en dos partes: en la primera estudiamos los llamados problemas en congruencias y la segunda está dedicada a distintas cuestiones relacionadas con sucesiones de números. A continuación discutiré brevemente qué tipo de problemas o técnicas aparecerán en los siguientes capítulos, sin entrar en detalle en los antecedentes o situación actual de cada problema ya que cada capítulo cuenta con una introducci'on detallada en la que se presentan y comentan los resultados en detalle.

La mayoría de los resultados que se presentan, especialmente aquellos incluidos en el Capítulo 2, dependen fuertemente de varios resultados complementarios, en ocasiones resultados clásicos y bien conocidos, que se han incluido en el Appéndice A al final del manuscrito.

◂ Problemas en congruencias ▸

Una gran parte de mi trabajo está dedicada al estudio de las distribución de soluciones a problemas en congruencias. La cuestión se reduce esencialmente a obtener estimaciones no triviales para la cantidad

$$|\{\mathbf{x} = (x_1, \dots, x_k) : f(x) \equiv 0 \pmod p\} \cap B|, \tag{4}$$

donde f es una función suficientemente buena (polinomial, exponencial,etc.) y B es el producto directo de intervalos -una caja- dentro del grupo abeliano en el que se encuentran las soluciones.

Esta clase de problemas ha sido intensamente estudiado y ha dado lugar a la aparición de matemáticas muy interesantes en el camino. Pensemos, por ejemplo, en los puntos afines de una variedad algebraica

$$V: \quad f_j(x_1, \dots, x_n) \equiv 0 \pmod p, \quad j = 1, \dots, m.$$

Uno desearía que los puntos de V estuvieran bien distribuidos en el cubo $[1, p]^n$, pero para una caja dada B ¿coincide el número de puntos $|V \cap B|$ con el valor esperado? En otras palabras: ¿podemos asegurar que

$$|V \cap B| = \frac{|B|}{p^n}|V|(1 + o(1))?$$

Es evidente que cuando el tamaño de la caja es demasiado pequeño uno no puede esperar obtener ningún tipo de resultado asintótico, ya que el número esperado de puntos puede no llegar siquiera a uno. Incluso cuando la caja es sustancialmente mayor, uno no tiene en general una asintótica de este tipo debido a restricciones geométricas (véase [44] para una discusión más detallada y ejemplos). Sin embargo, en muchas situaciones interesantes uno puede probar la equidistribución de las soluciones en (4). Véase por ejemplo [45, 73, 97].

Dichos resultados de distribución se han obtenido tradicionalmente mediante las técnicas clásicas en sumas exponenciales y sumas de caracteres, que en la mayoría de los casos dependen de resultados profundos de Geometría Algebraica -relacionados con la llamada Hipótesis de Riemann para curvas o variedades- pero en algunos casos se pueden deducir de ciertas propiedades aditivas de los conjuntos de puntos en cuestión. De hecho, dado cualquier conjunto A para obtener buenas estimaciones para la distribución de puntos en A es suficiente probar que -para al menos un gran número de caracteres ψ- se tiene

$$\left|\sum_{a\in A}\psi(a)\right| \ll |A|^{1/2}. \tag{5}$$

Es sencillo comprobar que para cualquier conjunto A en un grupo abeliano se cumple lo siguiente:

$$|A|^{1/2} \ll \max_{\psi\neq\psi_0}\left|\sum_{a\in A}\psi(a)\right| \leq |A|.$$

Lo que significa que la cota en (5) es esencialmente la mejor posible. Muchas de las obstrucciones geométricas que aparecen en este problema pueden ser traducidas a este lenguaje: el conjunto que nos interesa ha de estar *bien distribuido en los caracteres del grupo*. Dedicaremos la Sección 1.2 a encontrar numerosos ejemplos de conjuntos que satisfacen esta propiedad.

Las estimaciones asintóticas para la cantidad en (4) son no triviales hasta un cierto umbral en el tamaño de B que, debido al uso de las técnicas clásicas en sumas exponenciales, incluye un factor logarítmico. El Capítulo 1 incluye los resultados de [32], donde mejoramos el término de error en estas estimaciones para una clase general de problemas en congruencias, logrando extender el rango para una fórmula asintótica como resultado. Las demostraciones están basadas en las ideas de Garaev [46] y Cilleruelo [21]. Los resultados se presentan de forma muy general y las pruebas combinan tanto argumentos combinatorios como las técnicas clásicas en sumas exponenciales.

El hecho de estudiar este problema en un contexto tan general nos permite aplicar el mismo a otra cuestión diferente. En la Sección 1.3 se emplean argumentos similares para resolver un problema aditivo en cuerpos finitos con potencias de elementos con un orden multiplicativo grande. Para un cuerpo finito $\mathbb{F}_q$, estudiamos condiciones suficientes que garanticen que el conjunto $\{\theta_1^x+\theta_2^y:\ 1\leq x\leq M_1,\ 1\leq y\leq M_2\}$ representa todos los elementos de $\mathbb{F}_q^*$. También investigamos el mismo problema para el conjunto de diferencias $\theta_1^x-\theta_2^y$ y, como consecuencia, probamos que todo elemento en $\mathbb{F}_q$ tiene una representación de la forma: $\theta^x-\theta^y$, $1\leq x,y\leq \sqrt{2}q^{3/4}$ siempre que θ tenga orden multiplicativo al menos $\sqrt{2}q^{3/4}$.

Este resultado mejora las anteriores cotas conocidas para una cuestión propuesta por A. Odlyzko, aunque la respuesta actual sigue estando muy lejos de la conjetura del propio Odlyzko.

La prueba de nuevo combina argumentos clásicos de sumas exponenciales con argumentos combinatorio-aditivos basados en la estructura de ciertos conjuntos de Sidon y se pueden encontrar en [31].

En el Capítulo 2 nos centramos en el problema de estimar la cantidad definida en (4) cuando la caja B es considerablemente más pequeña. Como dijimos anteriormente, por debajo de cierto umbral no es posible obtener una fórmula asintótica. En particular, para estas cajas *pequeñas* uno sólo puede estudiar la concentración de soluciones y derivar buenas cotas superiores para el número de puntos que caen en dicha caja. Esta cuestión fue introducida por Cilleruelo y Garaev [22] en el caso particular de la hipérbola modular y después en [23] se han obtenido una serie de resultados generales en esta dirección. En este caso, las técnicas clásicas de sumas exponenciales no son adecuadas y uno debe explotar argumentos de la Combinatoria Aditiva poder mejorar la cota trivial en este rango.

En la Sección 2.1 se presentan cotas superiores para el número de soluciones

$$Q(x, y) \equiv 0 \pmod{p}, \quad (x, y) \in B,$$

donde $Q \in \mathbb{Z}[X, Y]$ es un polinomio cuadrático absolutamente irreducible (modulo p) con discriminante no nulo. Este resultado, que generaliza el resultado principal de [22], fue publicado en [103] y se presenta aquí como aperitivo para las siguientes secciones del Capítulo 2.

El resto del capítulo combina los resultados obtenidos en [16] y [28]. En particular, se estudia este problema para una clase general de curvas

$$(x, y): \quad f(x) \equiv y \pmod{p} \quad \text{o} \quad f(x) \equiv y^2 \pmod{p}, \quad f \in \mathbb{Z}[x].$$

En muchos casos obtenemos estimaciones no triviales y mejoramos algunas de las cotas anteriormente conocidas. Para ciertos rangos de los parámetros involucrados, cuando la caja es muy pequeña, nuestros resultados son óptimos y deberían ser considerados como análogos módulo p de los resultados de Bombieri y Pila [8] sobre el número de puntos enteros en curvas planas.

Las pruebas incluidas en las Secciones 2.2-2.4 dependen profundamente de la conexión que existe entre el problema de distribución de puntos en cajas pequeñas en curvas modulo p con la delicada combinación de resultados de la Geometría de los Números, la teoría de aproximación Diofántica, el teorema del valor medio de Vinogradov así como de el método de Weyl.

Los resultados aquí descritos no sólo son profundos, interesantes y sorprendentemente generales, sino que también tienen intersantes aplicaciones. Éstas han sido incluidas en la Sección 2.4 y van desde el estudio de clases de isomorfía de curvas hiperelípticas en ciertas familias *finas* a el diámetro de trayectorias parciales de sistémas dinámicos módulo p.

Por desgracia, nuestros resultados no cubren todos los rangos de $|B|$. El ataque a este problema desde los métodos de la Combinatoria Aditiva parece ser el más adecuado y fructífero cuando las cajas son pequeñas, mientras que para cajas grandes los métodos clásicos de sumas exponenciales son eficaces, pero tan sólo hasta cierto umbral en el tamaño de la caja. Pensemos, por ejemplo, en los puntos de una curva elíptica definida por la ecuación

$$E_{a,b}: \quad y^2 \equiv x^2 + ax + b \pmod{p}.$$

Cuando consideramos el número de puntos en un cuadrado $(x, y) \in B$, se conocen:

▸ Resultados asintóticos: $|E_{a,b} \cap B| \sim |B|/p$ si $|B| = \omega(p^{3/2})$.

Gracias a los métodos de geometría algebraica y a las técnicas clásicas en sumas exponenciales. Estos resultados nos permiten llegar a cotas no triviales siempre que $|B| \gg p$.

▸ Cotas superiores óptimas: $|E_{a,b} \cap B| \ll |B|^{1/6+o(1)}$ si $|B| \leq p^{2/9}$.

Estas se obtienen via métodos de la combinatoria aditiva. De hecho, mediante distintos enfoques somos capaces de obtener cotas no triviales para esta cantidad (es decir $o(|B|^{1/2})$) hasta $|B| = o\left(p^{2/3}\right)$.

Esto quiere decir que, en el rango $p^{2/3-\epsilon} \leq |B| \ll p$, nuestros métodos no son suficientemente buenos. Recientemente, Chang [15] obtuvo cotas no triviales del tipo $|B|^{1/2-\epsilon}$ para esta cantidad en un rango ligeramente mayor: $p^{\epsilon} \leq |B| \leq p^{18/23}$. Sin embargo, sigue existiendo un intervalo para el que no se conoce ninguna cota no trivial. Parece que ni las sumas exponenciales ni las técnicas de combinatoria aditiva son suficientemente eficientes en este rango. Sería muy interesante encontrar un método o desarrollar técnicas para lidiar con el problema en este rango intermedio.

Obsérvese que estos problemas tienen una generalización natural a cuerpos finitos. En vez de considerar curvas o valores de polinomios en cuerpos primos, si uno mueve el problema a un cuerpo finito arbitrario $\mathbb{F}_q$ entonces la generalización natural de un intervalo sería un espacio afín. Esta cuestión ha sido recientemente estudiada en varios trabajos [27, 86, 83].

▸ Sucesiones de números ◂

El resto del trabajo presentado aquí tiene un protagonista común: sucesiones de números naturales. De hecho, no todos los problemas que discutiremos se refieren a sucesiones sino más bien a conjuntos finitos de números, pero los resultados son en cualquier caso asintóticos en el número de elementos del conjunto.

▸ El mínimo común múltiplo de una sucesión:

En el Capítulo 3 estudiamos el crecimiento del mínimo común múltiplo de ciertas sucesiones de enteros. En particular, estudiamos el comportamiento asintótico de la siguiente función

$$\psi(S) = \log \operatorname{lcm}\{a : a \in S\},$$

para distintas familias de conjuntos S. Esta función es una generalización natural de la clásica función de Chebishev $\psi(n)$, cuyo estudio y comprensión fue esencial en la prueba del Teorema del Número Primo. Este capítulo presenta dos versiones completamente distintas de entender la función ψ, que de alguna manera encapsula -al menos cuantitativamente- la información aritmética de un conjunto S de números naturales.

En la Sección 3.1 estudiamos la asintótica de esta función para la sucesión $1^2 + 1, 2^2 + 1, \ldots, n^2 + 1$. Usando un resultado de Homma sobre la distrubución de raíces de polinomios cuadráticos modulo primos, calculamos el término de error para la asintótica que obtuvo Cilleruelo [20]. Las pruebas explotan argumentos clásicos de teoría analítica de números y

hacen un estudio detallado del método que introdujo Cilleruelo para sucesiones cuadráticas generales. Los resultados de esta sección han sido publicados en [99].

La Secciíon 3.2 se centra en el estudio de la cantidad $\psi(S)$ para un conjunto aleatorio $S \subseteq [n]$ considerando dos modelos probabilísticos diferentes, que son análogos a los modelos $G(n,p)$ y $G(n,M)$ de grafos aleatorios.

En el primer modelo, para cada elemento de $m \in [n]$ se escoge su pertenencia al conjunto S de forma aleatoria e independiente con cierta probabilidad fija $\delta = \delta(n)$. En el segundo modelo, restringimos nuestra atención a los k-subconjuntos de $[n]$ (donde $k = k(n)$) escogiendo de entre los $\binom{n}{k}$ posibles subconjuntos de forma uniforme. En ambos casos, obtenemos una fórmula asintótica para la variable aleatoria $\log(\operatorname{lcm}[S])$ que se cumple asintóticamente casi siempre cuando $n \to \infty$. Por ejemplo, demostramos que para casi todos los conjuntos $S \subseteq \{1,\dots,n\}$: $\operatorname{lcm}\{a : a \in S\} = 2^{n(1+o(1))}$.

Comparamos los resultados aleatorios obtenidos con resultados previos de Cilleruelo [20] en el mcm de valores de una sucesión polinomial y, en particular, los obtenidos con respecto al polinomio estudiado en la Sección 3.1. Por ejemplo, el término principal en la fórmula asintótica de Cilleruelo

$$\log \operatorname{lcm}\left\{k^2+1 : k \le \sqrt{n}\right\} = \frac{1}{2}\sqrt{n}\log n + c\sqrt{n} + o\left(\sqrt{n}\right)$$

coincide con el valor $\log \operatorname{lcm}[S]$ para casi todo conjunto S escogido de aleatoria entre los conjuntos $\{1,2,...,n\}$ de tamaño $[\sqrt{n}]$ de forma uniforme, sin embargo aparece una diferencia en el término secundario.

Esta Sección contiene los resultados de [30], cuyas pruebas involucran probabilidad elemental así como teoría de los números primos.

▸ Dígitos no nulos de sucesiones combinatorias:

Fijado $b \ge 2$ un entero positivo y S una sucesión infinita de enteros. Si la sucesión tiene algún significado combinatorio, es natural preguntarse cómo pueden llegar a ser las representaciones de sus elementos en base b. En el Capítulo 4 estudiamos el siguiente problema: para una sucesión S con un crecimiento dado, ¿cuán a menudo los elementos de S pueden escribirse con un pequeño número de dígitos? Esta cuestión ha sido estudiada anteriormente para sucesiones combinatorias bien conocidas como $n!$ [69], números de Fibonacci [93] o números de Catalan [72], por ejemplo.

En este caso, segimos una estrategia muy general para demostrar para una gran variedad de sucesiones $\{a_n\}_{n=1}^{\infty}$ que para casi todo n la suma de los dígitos de a_n en base b es al menos $c_b \log n$, donde c_b es una constante que depende de b y la propia sucesión. Nuestro enfoque cubre varias sucesiones que provienen de la teoría de números y la combinatoria y sólo depende del crecimiento de la sucesiíon, no de restricciones aritméticas o una formulación recursiva.

De hecho, demostramos que el enunciado anterior se cumple para cualquier sucesión $\{a_n\}_{n=1}^{\infty}$, con un crecimiento del tipo

$$a_n = e^{f(n)}\left(1 + O\left(n^{-\alpha}\right)\right), \ \alpha > 0 \tag{6}$$

donde f es una función dos veces diferenciable que ha de satisfacer $f''(x) \asymp 1/x$, al menos para x suficientemente grande. El número de permutaciones, involuciones, árboles de Cayley o grafos en superficies, entre otros, satisfacen esta condición de crecimiento.

Dedicamos la Sección 4.1 a demostrar que la sucesión de los números de Bell satisface la condición (6) de crecimientorequerida. En este caso, el análisis es más intrincado debido a que las estimaciones conocidas para el enésimo número de Bell dependen de cierta función de n definida de forma implícita.

Los resultados que incluyen este capítulo han sido publicados en [25].

- g-Bases para intervalos de enteros:

Hay muchos problemas clásicos relacionados con distintas restricciones impuestas sobre la función de representación

$$r_A(x) = |\{(a, a') \in A \times A : \ a + a' = x\}|,$$

para conjuntos o sucesiones A.

Buenos ejemplos de este hecho son los llamados conjuntos de Sidon, $r_A(x) \leq 2$, o las bases aditivas, $r_A(x) \geq 1$, que pueden ser etudiados en contextos diferentes (grupos finitos, grupos infinitos, semigrupos, intervalos, etc.) dando lugar a cuestiones totalmente distintas.

En el Capítulo 5 estudiamos la mínima cardinalidad posible de g-bases para intervalos, es decir A ha de cumplir $r_A(x) \geq g$ para todo $x \in \{1, \dots, n\}$. Sea

$$\gamma_g(n) = \min_{A \subset \mathbb{Z}} \{|A| : \ A \text{ is a } g - \text{basis for } \{1, \dots, n\}\}.$$

Está claro que dicho mínimo existe y es sencillo comprobar que la cantidad $\gamma_g(n)$ tiene orden $\sqrt{gn}$.

El objetivo de este capítulo es estudiar las cantidades

$$\underline{\gamma_g} = \liminf_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}} \quad \text{and} \quad \overline{\gamma_g} = \limsup_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}}$$

y demostrar que sus límites en g coinciden. De hecho, demostramos que el valor de dicho límite depende de la norma de ciertas funciones positivas y finitamente soportadas, que tienen integral pequeña y autoconvolución grande en un intervalo fijo. La estrategia sigue las lineas de [26], donde se estudia este problema para conjuntos g-Sidon en intervalos (es decir $r_A(x) \leq g$ para todo $x \in \{1, \dots, n\}$) y se aborda el problema considerando sucesivas construcciones de conjuntos con soporte restringido.

Para poder probar esto hemos de explotar buenas construcciones -basadas en las ideas de [88]- de conjuntos en grupos finitos cuya función de representación está *próxima* a ser constante. Dichas construcciones están incluidas en la Sección 5.1, así como algunas consideraciones sobre conjuntos en grupos finitos con función de representación restringida.

Siguiendo las ideas de Cilleruelo, Ruzsa y Vinuesa [26], relacionamos las construcciones discretas para g-bases con funciones positivas y de soporte compacto cuya autoconvolución

está inferiormente acotada en un intervalo fijo. En la sección 5.2 mostramos cómo conectar el problema de construir una función con ciertas propiedades de autoconvolución a partir de un conjunto con propiedades análojas en su función de representación. Finalmente, en la Sección 5.1 obtenemos un conjunto cuya función de representación replica las propiedades de autoconvolución de una función dada.

Los resultados incluidos en esta tesis se pueden encontrar en los siguientes artículos de investigación publicados o preprints:

[16] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, Points on curves in small boxes and applications, *Michigan Math. J.*, 63(3):505–534, 2014.

[25] J. Cilleruelo, F. Luca, J. Rué and A. Zumalacárregui, On the sum of digits of some sequences of integers, *Cent. Eur. J. of Math.* 11(1): 188–195, 2013.

[28] J. Cilleruelo, I. E. Shparlinski y A. Zumalacárregui, Isomorphism classes of elliptic curves over a finite field in some thin families, *Math. Res. Lett.*, 19(2):335–343, 2012.

[30] J. Cilleruelo, P. Šarka, J. Rué, and A. Zumalacárregui, The least common multiple of sets of positive integers, *J. Number Theory* 144:92–104, 2014.

[29] J. Cilleruelo, C. Vinuesa and A. Zumalacárregui, Representation functions in finite groups and bases for intervals, *preprint*, 2014.

[31] J. Cilleruelo and A. Zumalacárregui, An additive problem in finite fields with powers of elements of large multiplicative order, *Rev. Mat. Complut.*, 27(2):501–508, 2014.

[32] J. Cilleruelo and A. Zumalacárregui, Saving the logarithm factor in the error term estimates of some congruence problems, *preprint*, 2014.

[99] J. Rué, P. Šarka and A. Zumalacárregui, On the error term of the logarithm of the lcm of a quadratic sequence, *J. de Théor. Nombres Bordeaux* 25(2):457–470, 2013.

[103] A. Zumalacárregui, Concentration points on modular quadratic forms, *Int. J. of Number Theory*, 7(7): 1835–1839, 2011.

Notation

Throughout this manuscript we used, indistinctly, Landau (o and O) and Vinogradov ($\ll$ and $\gg$) notations. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to the statement that $|U| \leq cV$ for some constant $c > 0$. Generally, the quantities U and V will depend (explicit or implicitly) on a parameter n. The constant c in the previous notation must be independent of n, but may occasionally depend, when obvious, on some other parameters but is absolute otherwise. We recall that the notations $U = o(V)$ and $V = \omega(U)$ imply that $\lim U/V = 0$ when $n \to \infty$. Observe that, when we write $U = V^{o(1)}$ we are claiming that for every positive ϵ, there exists a constant C_ϵ, which must be independent of n, such that $U \leq C_\epsilon V^\epsilon$.

In the following chapters $\mathbb{N}$ will denote the set of natural numbers, $\mathbb{Z}$ the set of integers, $\mathbb{Q}$ rational and $\mathbb{R}$ real numbers. For a natural number n, we denote by $[n]$ the set consisting of $\{1, \ldots, n\}$ and by $\binom{[n]}{k}$ the set of all subsets of $[n]$ of exactly k elements. $\mathbb{Z}_n$ will denote the cyclic group $\mathbb{Z}/n\mathbb{Z}$ and will often be represented by the classes $\{0, 1 \ldots, n-1\}$. An interval on a cyclic group $\mathbb{Z}_n$, or an interval modulo n, will be nothing but a set consisting of certain residue classes modulo n which correspond to consecutive integers and will be denoted $I = [b+1, b+M] = \{b+1, \ldots, b+M\} \subseteq \mathbb{Z}_n$. A box B is the direct product of intervals, in certain abelian group direct product of cyclic groups, and we say that B is a cube (resp. a square) when all intervals have the same size. For a finite set A we will denote by $|A|$ its cardinality.

To simplify the notation related to exponential sums we will use the traditional notation $e(x) = e^{2\pi i x}$. A general Abelian group will be denoted by $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. Additive characters of an abelian group G will be denoted by ψ and indexed by their coefficients: for a given $\alpha \in G$, the additive character ψ_α acts on a given element $\mathbf{x} = (x_1, \ldots, n_k)$

$$\psi_\alpha(x) = e\left(\tfrac{\alpha_1 x_1}{n_1} + \cdots + \tfrac{\alpha_k x_k}{n_k}\right).$$

The trivial character will be denoted by ψ_0.

In general, unless otherwise specified, p will denote a prime number and the finite field of p elements will be denoted by $\mathbb{F}_p$. The letter q will be reserved to prime numbers or powers of prime numbers. Multiplicative characters will be generally denoted by χ and the trivial character by χ_0.

For subsets A, B of an abelian group or semigroup, we define the representation function

$$r_{A+B}(x) = |\{(a, b) \in A \times B : \ a + b = x\}|.$$

And denote by $r_A(x) = r_{A+A}(x)$ the representation function of a set and, analogously, $d_A(x) = r_{A-A}(x)$.

The letter δ will denote a probability value in $[0, 1]$ and might depend, when specified, on certain parameter n, $\mathbb{P}(E)$ and $\mathbb{E}(X)$ will denote probability of certain event E and expectation of a random variable X.

For a given real valued function f we will denote its autoconvolution at a point $x \in \mathbb{R}$

$$(f * f)(x) = \int f(t)f(x-t)dt.$$

As usual, $\|f\|_1$ will denote its L^1-norm. For a real number x we denote, as usual, by $\|x\|$ the nearest integer to x, by $\lfloor x \rfloor$ is the largest integer not greater than x (the floor of x), by $\lceil x \rceil$ is the smallest integer not less than x and by $\{x\} = |x - \|x\||$ the fractional part of x.

Part I

Congruence problems

▼

Distribution and concentration results

for solutions lying in a box

Chapter 1

Distribution of solutions to congruences: large boxes

The use of exponential sum techniques is one of the cornerstones of modern analytic number theory. The proof of the Riemann hypothesis by Weil for curves, by Deligne for general varieties, provides fantastic tools to solve problems from number theory.

Exponential sums are the natural, and sometimes the only, approach to study the equidistribution of values of polynomials in intervals and equidistribution of solutions to a given congruence of the type

$$\begin{cases} f(x_1,\dots,x_n) \equiv 0 \pmod p, \\ H_i + 1 \le x_i \le H_i + M_i,\ i = 1,\dots,n, \end{cases}$$

where f is some interesting function (polynomial, exponential, etc.). These two problems can be formulated in terms of certain *interesting* sets A (plane curves or more general algebraic sets, values of polynomials or Sidon sets, for example) in an abelian group G and the number of incidences of these sets with a given box $B = \prod_i [H_i + 1, H_i + M_i] \subseteq G$. In this case, we say that a set A is well distributed -or equidistributed- in G if for every sufficiently large box B the set A satisfies

$$|A \cap B| \sim \frac{|A||B|}{|G|}.$$

It follows from the orthogonality of the characters ψ of an abelian group G, that

$$|A \cap B| = \frac{1}{|G|} \sum_{\psi} \sum_{a \in A} \sum_{b \in B} \psi(a-b).$$

If we separate the contribution of the trivial character from the rest we will obtain the desired main term plus some error term that we must bound, namely

$$|A \cap B| = \frac{|A||B|}{|G|} + \frac{1}{|G|} \sum_{\psi \neq \psi_0} \sum_{a \in A} \sum_{b \in B} \psi(a-b). \tag{1.1}$$

Whenever the last sum -*i.e.* error term- in (1.1) is proven to be $o(|A||B|/|G|)$ we have an asymptotic for $|A \cap B|$ and we can say that "*A is equidistributed in G*". The range in $|B|$ for which we obtain an asymptotic for this quantity will depend on how well we estimate the error term in (1.1) and on the properties of the set A.

The usual method to handle sums of this type, which in the end are running over the set $A \cap B$, is to convert them into sums of the following kind and estimate them:

$$x \left| \frac{1}{|G|} \sum_{\psi \neq \psi_0} \sum_{a \in A} \sum_{b \in B} \psi(a-b) \right| \leq \frac{|\widehat{A}|}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{b \in B} \psi(-b) \right|,$$

where

$$|\widehat{A}| = \max_{\psi \neq \psi_0} \left| \sum_{a \in A} \psi(a) \right|.$$

This is achieved via the following well known result.

Lemma 1 (Vinogradov)**.** *For every $M \geq 1$ and every positive integer $n > 1$ we have*

$$\sum_{\alpha=1}^{n-1} \left| \sum_{x=1}^{M} e\left(\tfrac{\alpha x}{n}\right) \right| < n \log n.$$

Therefore, if $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ the error term in (1.1) is

$$\ll_k |\widehat{A}| \log^k (|G|).$$

Observe that the above error term is given in terms of $|\widehat{A}|$, so we must obtain good estimates for this quantity. It is easy to check that $|A|^{1/2} \leq |\widehat{A}| \leq |A|$, but in most applications A is a set with $|\widehat{A}| \ll |A|^{1/2}$.

Consider, for example, the modular hyperbola

$$A_1 = \{(x, y) : xy \equiv \lambda \pmod{p}\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$$

and the box $B = [x_0 + 1, x_0 + M] \times [y_0 + 1, y_0 + M]$. The usual techniques on character sums (see for example [56]) show that, for $\lambda \not\equiv 0 \pmod{p}$,

$$|A_1 \cap B| = \frac{|B||A_1|}{|G|} + O\big(p^{1/2} \log^2 p\big), \tag{1.2}$$

which provides the asymptotic formula $|A_1 \cap B| \sim |B|/p$ in the range

$$|B| p^{-3/2} \log^{-2} p \to \infty.$$

This result was improved by Garaev [46], who obtained the error term

$$O(p^{1/2} \log^2(|B|^{1/2} p^{-3/4} + 3))$$

and therefore extended the range for an asymptotic formula up to $|B| p^{-3/2} \to \infty$.

Other example is the exponential congruence given by the set

$$A_2 = \{(x, y) : g^x - g^y \equiv 1 \pmod p\} \subset \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$$

and the box $B = [1, M]^2$, where g is a primitive root of $\mathbb{F}_p^*$. As in the previous example, it is well known that, for $\lambda \not\equiv 0 \pmod p$,

$$|A_2 \cap B| = \frac{|A_2||B|}{|G|} + O\big(p^{1/2} \log^2 p\big), \tag{1.3}$$

which also provides the asymptotic formula $|A_2 \cap B| \sim |B|/p$ in the range $|B|p^{-3/2} \log^{-2} p \to \infty$. Garaev [46] obtained the error term

$$O(|B|^{1/3} \log^{2/3}(|B|^{1/2} p^{-3/4} + 3) + p^{1/2}), \tag{1.4}$$

extending the range for an asymptotic formula up to $|B|p^{-3/2} \to \infty$. The same range for the asymptotic formula was obtained by Cilleruelo [21] by showing that the error term was $O(4^r p^{1/2}((|B|p^{-3/2})^{1/r} + 1))$, for any positive r. Garaev's proof exploits character sums arguments and works in $\mathbb{Z}_p$, while Cilleruelo's proof is combinatorial and works on the group $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, where the elements of A_2 live.

The combination of the ideas in [46] and [21] allow us to improve both error terms in (1.2) and (1.3), and, which is more interesting, to obtain a general result which saves the logarithmic factor in many similar situations.

Theorem 1. *Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, $A \subseteq G$ and B a k-dimensional box in G. Then*

$$|A \cap B| = \frac{|A||B|}{|G|} + \theta |\widehat{A}| \left(1 + \log_+^k \left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right),$$

for some $|\theta| \le 100^k$, where $\log_+(x) = \max\{0, \log x\}$.

Nevertheless, since it is a very general result, we will dedicate Section 1.2 to some of the possible applications, analysing the quantity $|\widehat{A}|$ in many interesting situations.

In some cases, good bounds for the quantity $|\widehat{A}|$ rely on very deep results, this is the case of the set A_1 considered in the congruence $xy \equiv \lambda \pmod p$, where Kloosterman sums appear. In these cases we will also need results on the number of points in varieties over finite fields and explicit bounds for several exponential sums, see Appendix A for more details.

In some interesting situations the set A in Theorem 1 is a dense Sidon set in G: differences $a - a' : \ a \neq a', \ a, a' \in A$ are all distinct and satisfies $|A| \ge |G|^{1/2} - O(1)$. In Proposition 1 we show that $|\widehat{A}| = O(|A|^{1/2})$ for these sets. The set A_2 considered before is an example of a dense Sidon set and Theorem 1 gives an improvement on previous estimates of Garaev and Cilleruelo for the error term in this problem (see Section 1.2.1).

We dedicate the last section of this chapter, Section 1.3, to a slightly different problem related to a question of A. Odlyzko: how big must be M to guarantee that every element in $\mathbb{F}_p$ has a representation of the form $g^x - g^y$ if both x and y are in $[1, M]$ and g is a primitive root modulo p? Exploiting similar ideas and techniques we improve the previous known bounds for this question and, in fact, we prove a more general result considering the problem in general finite fields with powers of elements of large multiplicative order.

Theorem 4. *Let θ_1, θ_2 be two elements of $\mathbb{F}_q$. If*

$$\min(ord_q(\theta_1), \lfloor M_1/2 \rfloor) \cdot \min(ord_q(\theta_2), \lfloor M_2/2 \rfloor) \geq q^{3/2},$$

then

$$\begin{aligned}\mathbb{F}_q^* \subseteq &\{\theta_1^x + \theta_2^y : 1 \leq x \leq M_1,\ 1 \leq y \leq M_2\},\\ \mathbb{F}_q = &\{\theta_1^x - \theta_2^y : 1 \leq x \leq M_1,\ 1 \leq y \leq M_2\}.\end{aligned}$$

We also take advantage of the symmetries of the problem in the case $\theta_1 = \theta_2$ and improve the result for the set of differences.

An important idea behind the proofs of these results relies on the fact that, when dealing with exponential sums, sometimes it is quite useful to introduce additional variables, which somehow smooth the problem. The next simple lemma will be very useful in the following proofs.

Lemma 2. *Let G be an finite abelian group. For any $A, B, C \subseteq G$ we have*

$$|\{ (b,c) \in B \times C : b + c \in A\}| = \frac{|B||C||A|}{|G|} + \theta \frac{|\widehat{A}|}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{b \in B} \psi(b) \right| \left| \sum_{c \in C} \psi(c) \right|,$$

for some $|\theta| \leq 1$, where

$$|\widehat{A}| = \max_{\psi \neq \psi_0} \left| \sum_{a \in A} \psi(a) \right|.$$

Proof. The number of pairs $(b,c) \in B \times C$ with $b + c \in A$ is given by

$$\frac{1}{|G|} \sum_{\psi} \sum_{A,B,C} \psi(b + c - a) = \frac{|B||C||A|}{|G|} + \text{Error},$$

where

$$\begin{aligned}|\text{Error}| &= \left| \frac{1}{|G|} \sum_{\psi \neq \psi_0} \sum_{A,B,C} \psi(b + c - a) \right| \\ &\leq \frac{1}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{a \in A} \psi(-a) \right| \left| \sum_{b \in B} \psi(b) \right| \left| \sum_{c \in C} \psi(c) \right| \\ &\leq \frac{|\widehat{A}|}{|G|} \sum_{\psi \neq \psi_0} \left| \sum_{b \in B} \psi(b) \right| \left| \sum_{c \in C} \psi(c) \right|.\end{aligned}$$

□

We will also need the following Corollary.

Corollary 1. *If $(B + B) \cap A = \emptyset$, then $|B| \leq |\widehat{A}||G|/(|A| + |\widehat{A}|)$.*

Proof. Setting $C = B$ in Lemma 2, we observe that the condition $(B + B) \cap A = \emptyset$ implies that

$$|B|^2|A| \leq |\widehat{A}| \sum_{\psi \neq \psi_0} \left| \sum_{b \in B} \psi(b) \right|^2 = |\widehat{A}| \sum_{\psi \neq \psi_0} \sum_{b,b' \in B} \psi(b - b') = |\widehat{A}|(|G||B| - |B|^2),$$

and the result follows. □

1.1 Asymptotic results: saving the logarithmic factor

The following theorem allows us to improve the error term on the asymptotic estimates obtained in many different problems. Such an improvement can be translated into the possibility of removing the logarithmic factor on the critical size of B, as in [46] was done for the sets A_1 and A_2.

Theorem 1. *Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, $A \subseteq G$ and B a k-dimensional box in G. Then*

$$|A \cap B| = \frac{|A||B|}{|G|} + \theta |\widehat{A}| \left(1 + \log_+^k \left(\frac{|B||A|}{|\widehat{A}||G|}\right)\right),$$

for some $|\theta| \leq 100^k$, where $\log_+(x) = \max\{0, \log x\}$,

$$|\widehat{A}| = \max_{\psi \neq \psi_0} \left| \sum_{a \in A} \psi(a) \right|$$

and the sum is taken over all non principal characters in G.

Before starting the proof, let us note that in order to profit from the previous result one would desire to have something close to $|\widehat{A}| \ll |A|^{1/2}$, but one could not expect such a thing in general. In fact not only one can find simple examples for which this bound does not hold, but also controlling the size of exponential sums in a large number of variables remains very difficult, since certain geometric conditions are almost impossible to check before applying the corresponding theorem, see [44, 61] for a more general discussion.

In Section 1.2.4, we illustrate how -following the same ideas- one can obtain a result analogous to Theorem 1, even if the quantity $|\widehat{A}|$ is big for a certain class of characters, and still save the logarithm factor on the range for an asymptotic result.

Proof. Let $B = \prod_{i=1}^k [H_i + 1, H_i + M_i]$, $1 \leq M_i \leq n_i$, be a k-dimensional box in $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. Consider the following approximations of B

$$B' = \prod_{i=1}^k [H_i + 1 - m_i, H_i + M_i], \quad B'' = \prod_{i=1}^k [H_i + 1, H_i + M_i - m_i],$$

for some suitable integers $m_i, 0 \leq m_i \leq M_i - 1$, to be chosen later. If we denote by $C = \prod_{i=1}^k [0, m_i]$, then it is clear that $B \subset B' + c$ for any $c \in C$, so each element $b \in B$ has at least $|C|$ representations of the form $b = b' + c$, $b' \in B'$, $c \in C$. In particular

$$|\{(b', c) \in B' \times C,\ b' + c \in A\}| \geq |A \cap B||C|.$$

Analogously, $B'' + c \subset B$ for any $c \in C$ and then

$$|\{(b'', c) \in B'' \times C,\ b'' + c \in A\}| \leq |A \cap B||C|.$$

Hence

$$\frac{|\{(b'', c) \in B'' \times C : b'' + c \in A\}|}{|C|} \leq |A \cap B| \leq \frac{|\{(b', c) \in B' \times C : b' + c \in A\}|}{|C|}.$$

In terms of Lemma 2 we have that

$$|A\cap B| \le \frac{1}{|C|}\Big(\frac{|A||B'||C|}{|G|}+\theta\frac{|\widehat{A}|}{|G|}\sum_{\psi\neq\psi_0}\Big|\sum_{B'}\psi(b')\Big|\sum_{C}\psi(c)\Big|\Big)$$
$$\le \frac{|A||B|}{|G|}+\frac{|A|\big(|B'|-|B|\big)}{|G|}+\frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B'}\psi(b')\Big|\sum_{C}\psi(c)\Big|, \tag{1.5}$$

and similarly

$$|A\cap B| \ge \frac{|A||B|}{|G|}-\frac{|A|\big(|B|-|B''|\big)}{|G|}-\frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B''}\psi(b'')\Big|\sum_{C}\psi(c)\Big|$$
$$\ge \frac{|A||B|}{|G|}-\frac{|A|\big(|B'|-|B|\big)}{|G|}-\frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B''}\psi(b'')\Big|\sum_{C}\psi(c)\Big|, \tag{1.6}$$

since $|B|-|B''|\le |B'|-|B|$.

Observe that, for a fixed character $\psi_\alpha,\ \alpha=(\alpha_1,\dots,\alpha_k)$, we have

$$\begin{aligned}\sum_{b'\in B'}\psi_\alpha(b') &= \prod_{i=1}^{k}\left(\sum_{b_i'=H_i+1-m_i}^{H_i+M_i} e\left(\tfrac{\alpha_i b_i'}{n_i}\right)\right)\\ \sum_{b''\in B''}\psi_\alpha(b'') &= \prod_{i=1}^{k}\left(\sum_{b_i''=H_i+1}^{H_i+M_i-m_i} e\left(\tfrac{\alpha_i b_i''}{n_i}\right)\right)\end{aligned} \tag{1.7}$$

and

$$\sum_{c\in C}\psi_\alpha(c)=\prod_{i=1}^{k}\left(\sum_{c_i=0}^{m_i} e\left(\tfrac{\alpha_i c_i}{n_i}\right)\right).$$

For a fixed i, each sum involved is a geometric sum with ratio $e(\alpha_i/n_i)$. Whenever $\alpha_i\neq 0$, if we choose α_i to be a representative with $|\alpha_i|\le n_i/2$, it is well known that for any a and m

$$\left|\sum_{x=a}^{a+m} e\big(\tfrac{\alpha_i x}{n_i}\big)\right| \le \frac{2}{|1-e\big(\frac{\alpha_i}{n_i}\big)|}\le\frac{4n_i}{|\alpha_i|},$$

and it is clear that, for any α_i including 0, this sum is bounded by $m+1$. To clear the exposition we will fix $\min\{4n_i/0, m+1\}:=m+1$ and include these two facts in the following estimate

$$\left|\sum_{x=a}^{a+m} e\big(\tfrac{\alpha_i x}{n_i}\big)\right| \le \min\left\{\tfrac{4n_i}{|\alpha_i|}, m+1\right\}, \tag{1.8}$$

where α_i is chosen to be the representative modulo n_i with minimum absolute value.

It follows from (1.7) and (1.8) that for every fixed $\alpha = (\alpha_1, \dots, \alpha_k) \in G,\ |\alpha_i| \le n_i/2$, the following estimates hold

$$\Big|\sum_{B'} \psi_\alpha(b')\Big| \le \prod_{i=1}^{k} \min\big\{\tfrac{4n_i}{|\alpha_i|}, M_i + m_i\big\} \le \prod_{i=1}^{k} \min\big\{\tfrac{4n_i}{|\alpha_i|}, 2M_i\big\},$$
$$\Big|\sum_{B''} \psi_\alpha(b'')\Big| \le \prod_{i=1}^{k} \min\big\{\tfrac{4n_i}{|\alpha_i|}, M_i - m_i\big\} \le \prod_{i=1}^{k} \min\big\{\tfrac{4n_i}{|\alpha_i|}, 2M_i\big\},$$
$$\Big|\sum_{C} \psi_\alpha(c)\Big| \le \prod_{i=1}^{k} \min\big\{\tfrac{4n_i}{|\alpha_i|}, m_i + 1\big\}.$$

Thus,

$$\begin{aligned}\sum_{\alpha} \Big|\sum_{B'} \psi_\alpha(b')\Big|\Big|\sum_{C} \psi_\alpha(c)\Big| &\le \sum_{\alpha} \prod_{i=1}^{k} \min\big\{\tfrac{4n_i}{|\alpha_i|}, 2M_i\big\} \min\big\{\tfrac{4n_i}{|\alpha_i|}, m_i + 1\big\} \\ &\le \prod_{i=1}^{k} \Big(\sum_{|\alpha_i| \le n_i/2} \min\big\{\tfrac{4n_i}{|\alpha_i|}, 2M_i\big\} \min\big\{\tfrac{4n_i}{|\alpha_i|}, m_i + 1\big\} \Big) \\ &\le \prod_{i=1}^{k} \Big(\sum_{0 \le \alpha_i \le n_i/2} \min\big\{\tfrac{8n_i}{\alpha_i}, 4M_i\big\} \min\big\{\tfrac{4n_i}{\alpha_i}, m_i + 1\big\} \Big)\end{aligned}$$

and the same upper bound holds for the sum in B''.

Observe that

$$\begin{aligned}&\sum_{0 \le \alpha_i \le n_i/2} \min\big\{\tfrac{8n_i}{\alpha_i}, 4M_i\big\} \min\big\{\tfrac{4n_i}{\alpha_i}, m_i + 1\big\} \\ &\quad = 4 \sum_{0 \le \alpha \le \frac{2n_i}{M_i}} M_i(m_i + 1) + 8 \sum_{\frac{2n_i}{M_i} < \alpha \le \frac{4n_i}{m_i+1}} \frac{n_i(m_i+1)}{\alpha} + 32 \sum_{\alpha > \frac{4n_i}{m_i+1}} \frac{n_i^2}{\alpha^2} \\ &\quad = S_1 + S_2 + S_3.\end{aligned}$$

To estimate the quantities S_i we use, for $2 \le A < B$ the inequalities

$$\sum_{A \le \alpha \le B} \frac{1}{\alpha} \le \log(2B/A) \quad \text{and} \quad \sum_{A < \alpha} \frac{1}{\alpha^2} \le \frac{2}{A},$$

and obtain

$$\begin{aligned}&S_1 \le 4M_i(m_i + 1)\left(\frac{2n_i}{M_i} + 1\right) \le 12n_i(m_i + 1), \\ &S_2 \le 8n_i(m_i + 1)\log\left(\frac{4M_i}{m_i + 1}\right) \le n_i(m_i + 1)\left(12 + 8\log\left(\frac{M_i}{m_i + 1}\right)\right), \\ &S_3 \le 16n_i(m_i + 1).\end{aligned}$$

Thus we have,

$$S_1 + S_2 + S_3 \le n_i(m_i + 1)\left(40 + 8\log\left(\frac{M_i}{m_i + 1}\right)\right) \tag{1.9}$$

and then

$$\sum_{\psi}\Big|\sum_{B'}\psi_\alpha(b')\Big|\Big|\sum_{C}\psi_\alpha(c)\Big| \le \prod_{i=1}^{k} n_i(m_i+1)\left(40+8\log\left(\frac{M_i}{m_i+1}\right)\right)$$

Combining the previous estimate we obtain the following bound for the last sum in (1.5)

$$\frac{|\widehat{A}|}{|G||C|}\sum_{\psi}\Big|\sum_{B'}\psi(b')\Big|\Big|\sum_{C}\psi(c)\Big| \le |\widehat{A}|\prod_{i=1}^{k}\left(40+8\log\left(\frac{M_i}{(m_i+1)}\right)\right), \tag{1.10}$$

since $n_1\cdot n_2\cdots n_k=|G|$ and $(m_1+1)\cdot(m_2+1)\cdots(m_k+1)=|C|$ by definition. The same bound applies to the sum in (1.6).

Observe that if $(x_1,\dots,x_k)\in B'\setminus B$, then $H_j+1-m_j\le x_j\le H_j$ for at least one $j\in\{1,\dots,k\}$. This implies

$$\begin{aligned}|B'|-|B| &\le \sum_{i=1}^{k}\Big(m_i\prod_{j\neq i}(M_j+m_j)\Big)\\ &= \sum_{i=1}^{k}\Big(\frac{m_i}{M_i+m_i}\prod_{j=1}^{k}(M_j+m_j)\Big) \le |B|2^k\sum_{i=1}^{k}\frac{m_i}{M_i}.\end{aligned} \tag{1.11}$$

Combining (1.5) and (1.6) with (1.10) and (1.11) we get

$$\left||A\cap B|-\frac{|A||B|}{|G|}\right| \le \frac{|A||B|2^k\sum_{i=1}^{k}\frac{m_i}{M_i}}{|G|}+|\widehat{A}|\prod_{i=1}^{k}\left(40+8\log\left(\frac{M_i}{(m_i+1)}\right)\right). \tag{1.12}$$

If $|B|>\frac{|\widehat{A}||G|}{|A|}$ we take

$$m_i=\left\lfloor M_i\frac{|\widehat{A}||G|}{|B||A|}\right\rfloor \le M_i-1,$$

and introduce it into (1.12) to get

$$\left||A\cap B|-\frac{|A||B|}{|G|}\right| \le |\widehat{A}|\left(k2^k+\left(40+8\log\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)^k\right).$$

If $|B|\le\frac{|\widehat{A}||G|}{|A|}$ we take $m_i=M_i-1$ and then we have

$$\left||A\cap B|-\frac{|A||B|}{|G|}\right| \le |\widehat{A}|\left(k2^k+40^k\right).$$

Using the notation $\log_+ x=\max(0,\log x)$ and the crude estimate $(A+B)^k\le 2^k(A^k+B^k)$, both inequalities can be bounded by

$$\begin{aligned}\left||A\cap B|-\frac{|A||B|}{|G|}\right| &\le |\widehat{A}|\left(k2^k+\left(40+8\log_+\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)^k\right)\\ &\le |\widehat{A}|\left(k2^k+2^k40^k+2^k8^k\log_+^k\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)\\ &\le \theta|\widehat{A}|\left(1+\log_+^k\left(\tfrac{|B||A|}{|\widehat{A}||G|}\right)\right)\end{aligned}$$

for some $\theta<100^k$. □

1.2 Applications

Once we are able to reduce the congruence problem to estimate the quantity $|A\cap B|$ for suitable $A, B \subset G$, we must be able to estimate $|\widehat{A}|$.

In our study, estimates for $|\widehat{A}|$ will follow from good bounds on sums of the form

$$\sum_{a\in A} \psi_\alpha(a) = \sum_{(x_1,\dots,x_n)\in A} e\left(\frac{\alpha_1 x_1 + \cdots + \alpha_k x_k}{p}\right), \tag{1.13}$$

where $A \subseteq G = \mathbb{F}_p^n$ may not be an algebraic variety but a more general set. Kloosterman sums are examples of this kind. But for more general finite abelian groups we will deal with sums of the form

$$\sum_{a\in A} \psi_\alpha(a) = \sum_{(x_1,\dots,x_n)\in A} e\left(\frac{\alpha_1 x_1}{n_1} + \cdots + \frac{\alpha_k x_k}{n_k}\right), \tag{1.14}$$

with $A \subseteq G = \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$. In both cases we will consider $\alpha = (\alpha_1,\dots,\alpha_k) \in G\backslash\{(0,\dots,0)\}$. Recall that some α_i might be zero but not all, and this would make a difference sometimes.

In some situations, good bounds for the quantities (1.13) and (1.14) rely on very deep results. That is the case of Weil's estimates for Kloosterman sums, which arised from the study of the structure of L-functions of algebraic varieties over finite fields and the so called Riemman Hypothesis for them. But sometimes these estimates are easy to obtain. That is the case of Sidon sets, which are studied in the following section.

1.2.1 Dense Sidon sets

A set $A \subset G$ is said to be a Sidon set if the differences $a - a' : \ a \neq a', \ a, a' \in A$ are all distinct in G. It is easy to obtain a trivial upper bound for the size of a Sidon set in G. Indeed if A is a Sidon set, then $|A - A| = |A|^2 - |A| + 1 \leq |G|$, since by definition every difference $a - a' = m \in A - A$ is distinct except from the element $0 \in A - A$, which is represented in exactly $|A|$ different ways. This gives $|A| \leq \sqrt{|G| - 3/4} + 1/2$ and there are examples where the equality holds. We will say that a Sidon set $A \subset G$ is dense if $|A| \geq |G|^{1/2} - O(1)$.

Good bounds for the quantity $|\widehat{A}|$ in this case follow easily from the additive properties of Sidon sets.

Proposition 1. *Let $A \subset G$ be a Sidon set with $|A| \geq |G|^{1/2} - O(1)$. Then,*

$$|\widehat{A}| = O\left(|A|^{1/2}\right).$$

Proof. For a set S, let $r_S(m)$ denote the number of representations of the element m as sum of two elements in S.

$$\Big|\sum_{a\in A}\psi(a)\Big|^2 = \sum_{a,a'\in A}\psi(a-a') = \sum_{m\in G} r_{A-A}(m)\psi(m) = \sum_{m\in G}(r_{A-A}(m)-1)\psi(m).$$

Since A is a Sidon set, we have that $r_{A-A}(m) \leq 1$ for $m \neq 0$ and $r_{A-A}(0) = |A|$. It follows from (1.2.1)

$$\Big|\sum_{a\in A}\psi(a)\Big|^2 = |A| - 1 - \sum_{m\notin A-A}\psi(m). \tag{1.15}$$

Thus we need to study the set $A - A$. It is clear that every pair (a, a'), $a, a' \in A$, uniquely determines the element $m = a - a'$, whenever $a \neq a'$, and the zero element is represented by every pair (a, a), $a \in A$. Therefore

$$|A - A| = |A|^2 - |A| + 1 \geq |G| - O(|A|),$$

since $|A| \geq |G|^{1/2} - O(1)$ by hypothesis. The previous equation implies that for a given character $\psi = \psi_\alpha$, we have

$$\Big| \sum_{m \notin A-A} \psi(m) \Big| \leq |G| - |A - A| = O(|A|).$$

Combining this bound with the expression in (1.15), we obtain the desired result

$$|\widehat{A}| = \max_{\psi \neq \psi_0} \Big| \sum_{a \in A} \psi(a) \Big| = O\big(|A|\big)^{1/2}.$$

□

Let us now apply Theorem 1 to dense Sidon sets. The following result follows directly from Proposition 1.

Corollary 2. *Let $A \subset G$ be a Sidon set with $|A| \geq |G|^{1/2} - O(1)$, and $B \subseteq G$ a k-dimensional box. Then*

$$|A \cap B| = \frac{|A||B|}{|G|} + O\left(|G|^{1/4}\left(1 + \log_+^k\left(|B||G|^{-3/4}\right)\right)\right).$$

In particular, $|A \cap B| \sim |A||B|/|G|$ when $|B||G|^{-3/4} \to \infty$.

Since the set $A_2 = \{(x, y) : g^x - g^y \equiv 1 \pmod p\}$ is a Sidon set of $p - 2$ elements in $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, it follows from the previous result that the number of solutions to the congruence

$$\begin{cases} g^x - g^y \equiv 1 \pmod p \\ (x, y) \in B = [1, M]^2 \end{cases}$$

is given by

$$|A_2 \cap B| = \frac{|B|}{p} + O\left(p^{1/2}\left(1 + \log_+^2\left(|B|p^{-3/2}\right)\right)\right).$$

Which improves the error term obtained by Garaev (1.4) and the one obtained by Cilleruelo.

The following result, which is a refinement form Proposition 1, will be required in Section 1.3.

Corollary 3. *Let g be a primitive root in the finite field $\mathbb{F}_q$, where q is a prime power, and let $A = \{(x, y) : g^x - g^y = \lambda\}$, then $|\widehat{A}| \leq q^{1/2}$.*

Proof. It follows from (1.15) that it is enough to study the set $A - A$. Observe that the $3(q - 2)$ elements of the form $(z, 0), (0, z)$ and (z, z), $1 \leq z \leq q - 2$ do not belong to $A - A$. Indeed, if $(z, 0) = (x + z, y) - (x, y)$ for some $(x + z, y), (x, y) \in A$ we would have that

$g^{x+z} - g^y = g^x - g^y = \lambda$, which is impossible unless $z \equiv 0 \pmod{q-1}$. The same argument applies to the elements of the form $(0, z)$ and (z, z).

Furthermore, since $|G| - |A - A| = |G| - (|A|^2 - |A| + 1) = 3(q-2)$, it follows that those are the only elements $m \notin A - A$. Therefore, for a given $\psi = \psi_{r,s}$, we have

$$\sum_{m \notin A-A} \psi(m) = \sum_{z=1}^{q-2} e\Big(\tfrac{rz}{q-1}\Big) + \sum_{z=1}^{q-2} e\Big(\tfrac{sz}{q-1}\Big) + \sum_{z=1}^{q-2} e\Big(\tfrac{(r+s)z}{q-1}\Big) \geq -3,$$

since every such sum is either -1 or $q-2$, depending on the values r and s.

Combining this bound with the expression in (1.2.1), we obtain the desired result

$$\Big|\sum_{a \in A} \psi(a)\Big| \leq \big(|A| + 2\big)^{1/2} = q^{1/2}.$$

□

In fact, the result remains true if one considers for any primitive roots g_1, g_2 of a finite field $\mathbb{F}_q$ the following sets:

$$A^-(g_1, g_2, \lambda) = \{(x, y) : g_1^x - g_2^y = \lambda \text{ in } \mathbb{F}_q\}, \tag{1.16}$$

$$A^+(g_1, g_2, \lambda) = \{(x, y) : g_1^x + g_2^y = \lambda \text{ in } \mathbb{F}_q\}, \tag{1.17}$$

which are Sidon sets in $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$. See Section 1.3 for details.

The case (1.16) for $g_1 \neq g_2$ can be reduced to Corollary 3. Let $\psi_{r,s}$ be the non trivial character $\psi(x, y) = e^{2\pi i(\frac{rx+sy}{q-1})}$ and t the integer such that $g_1^t = g_2$. We observe that $(x, y) \in A^-(g_1, g_2, \lambda)$ if and only if $(x, ty) \in A^-(g_1, g_1, \lambda)$. Then, for any $a = (x, y) \in A^-(g_1, g_2, \lambda)$ we have $\psi_{r,s}(x, y) = \psi_{r,st^{-1}}(x, ty)$. Thus

$$\max_{a \in A^-(g_1,g_2,\lambda)} |\psi_{r,s}(a)| = \max_{a \in A^-(g_1,g_1,\lambda)} |\psi_{r,st^{-1}}(a)| \leq q^{1/2}.$$

The case (1.17) is easier. It is clear that $(x, y) \in A^+(g_1, g_2, \lambda)$ if and only if $(x, y+(q-1)/2) \in A^-(g_1, g_2, \lambda)$ and that $\psi(a + (0, (q-1)/2)) = \psi(a)\psi(0, (q-1/2))$. Thus

$$\max_{a \in A^+(g_1,g_2,\lambda)} |\psi(a)| = \max_{a \in A^-(g_1,g_1,\lambda)} |\psi(a + (0, (q-1)/2))| \leq q^{1/2}.$$

1.2.2 Plane curves

Let us now consider sets of the form

$$C_f = \{(x_1, x_2) \,:\, f(x_1, x_2) \equiv 0 \pmod{p}\} \subset G = \mathbb{F}_p^2,$$

of roots of $f \in \mathbb{Z}[X_1, X_2]$ a polynomial in two variables. For these curves, Weil estimates for Kloosterman sums were generalized by Bombieri [7], who showed that, for any absolutely irreducible polynomial $f \in \mathbb{F}_p[x, y]$, of degree at most two, and any $(a, b) \neq (0, 0)$

$$\left|\sum_{(x,y) \in C_f} e\left(\tfrac{ax+by}{p}\right)\right| \ll p^{1/2}. \tag{1.18}$$

Observe that, in order to obtain results via Theorem 1 one should be able to estimate the number of points of C_f in first place. For example, if one considers polynomials given by $f(x,y) = x^3 + ax + b - y^2$, with nonzero discriminant, then C_f consists on the affine points of an elliptic curve and it follows from the Hasse bound that $|C_f| = p + 1 - t$ with $|t| < 2p^{1/2}$. In general, Weil and Lang (see Theorem 28) showed that if A is the set of affine points of any variety of dimension d

$$|A| = p^d \left(1 + o(1)\right). \tag{1.19}$$

Corollary 4. *Let p be a prime number, $f \in \mathbb{F}_p[x,y]$ an absolutely irreducible polynomial and $B \subseteq \mathbb{F}_p^2$ a two dimensional box. Then*

$$|C_f \cap B| = \frac{|B|}{p} + O\left(p^{1/2}\left(1 + \log_+^2\left(|B||p|^{-3/2}\right)\right)\right).$$

In particular, $|C_f \cap B| \sim |B|/p$ when $|B|p^{-3/2} \to \infty$.

Proof. It follows from Theorem 1, Equation (1.18) and Equation (1.19) for $d = 1$. □

1.2.3 Polynomial values

If one considers the set of all points

$$A_F = \{(f_1(t), f_2(t), \ldots, f_k(t)) : 1 \le t \le p\} \subset \mathbb{F}_p^k,$$

for some $F = (f_1, \ldots, f_k)$ with $f_i \in \mathbb{Z}[X]$. If the polynomials f_i are linearly independent modulo p, then it follows from the Weil bounds [100] that

$$\sum_{a \in A_F} e\left(\frac{\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k a_k}{p}\right) = \sum_{t=1}^{p} e\left(\frac{\alpha \cdot F(t)}{p}\right) \ll p^{1/2}, \tag{1.20}$$

where $\alpha \cdot F(t) = (\alpha_1, \ldots, \alpha_k) \cdot (f_1(t), \ldots, f_k(t)) = \alpha_1 f_1(t) + \alpha_2 f_2(t) + \cdots + \alpha_k f_k(t)$, and the constants implied depend only on the degree of $\alpha \cdot F$.

Corollary 5. *Let p be a prime and $F = (f_1, \ldots, f_k)$ with $f_i \in \mathbb{F}_p[x]$ linearly independent modulo p. For any k dimensional box $B \subseteq \mathbb{F}_p^k$*

$$|A_F \cap B| = \frac{|B|}{p^{k-1}} + O\left(p^{1/2}\left(1 + \log_+^k\left(|B|p^{1/2-k}\right)\right)\right).$$

In particular, $|A \cap B| \sim |B|/p^{k-1}$ when $|B|p^{1/2-k} \to \infty$.

Proof. The result follows from Theorem 1, Equation (1.20) and Theorem 28, on the number of points of a variety, which states that $|A_F| = p(1 + o(1))$. □

There are many examples of this kind. For example consider an hyperelliptic curve, given by a non-singular Weierstrass equation,

$$H_{\mathbf{a}}: \quad Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1 X + a_0,$$

where $\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathbb{F}_p^{2g}$.

Isomorphisms of hyper elliptic curves given by Weierstrass equations that preserve this form are given by $(x, y) \to (t^2 x, t^{2g+1} y)$ for some $t \in \mathbb{F}_p^*$. Thus two hyperelliptic curves $H_{\mathbf{a}}$ and $H_{\mathbf{b}}$ are isomorphic if there exists $t \in \mathbb{F}_p^*$ such that

$$a_i \equiv t^{4g+2-2i} b_i \pmod{p}, \qquad i = 0, \dots, 2g-1.$$

Thus, if $F(t) = (t^{4g+2-2i} b_i)$ for $i = 0, \dots 2g-1$ then $|A_F \cap B|$ will count the number of curves which are isomorphic to $H = H_{\mathbf{b}}$ and whose coefficients are in B. Let us denote this quantity by $N(H; B) = \#\{a \in B : H_{\mathbf{a}} \sim H\}$.

The standard application of the Weil bounds (see [62] for further details) gives that the number of curves which are isomorphic to a given one with coefficients in a box B is given by

$$N(H; B) = \frac{|B|}{p^{2g-1}} + O\left(p^{1/2} \log^{2g} p)\right),$$

and would provide an asymptotic for this quantity if $|B| p^{-2g+1/2} \log^{-2g} p \to \infty$. It follows from Corollary 5 that

$$N(H; B) = \frac{|B|}{p^{2g-1}} + O\left(p^{1/2} \left(1 + \log_+^{2g} \left(|B| p^{1/2-2g}\right)\right)\right).$$

Note that our result extends the range to $|B| p^{-2g+1/2} \to \infty$, saving once again the logarithm factor.

The quantity $N(H; B)$ will be studied in the next chapter (Section 2.4.1), obtaining upper bounds for qualitatively smaller boxes.

1.2.4 Multidimensional hyperbolas

Unfortunately, estimates of this kind cannot be generalized to higher dimensions. If one considers, for a general variety V, the sums

$$\sum_{a \in V} e\left(\frac{\alpha_1 x_1 + \dots + \alpha_k x_k}{p}\right),$$

one could not expect to obtain something like $O(p^{k/2})$ for all $\alpha \neq 0$ and a general class of polynomials for $k > 2$. In this case good bounds do not follow immediately from Deligne results [35] and one should impose either more concrete geometric restrictions (see [61] for examples in $k = 3$) or distinguish between different possible α's, see [62, Chapter 11] for further discussion.

Nevertheless, in some cases this difficulty can be overpassed. Let us focus on the n-dimensional hyperbola:

$$H_n = \{(x_1, \dots, x_{n+1}) : x_1 \cdots x_{n+1} \equiv 1 \pmod{p}\}. \tag{1.21}$$

In this case it is clear that non-trivial characters with zero coordinates will imply large character sums, but the number of such characters is small compared with the total number of characters.

Proposition 2. *Let p be a prime number and H_n the n-dimensional hyperbola defined by Equation* (1.21)*. Then,*

$$|\widehat{H}_{n,s}| = \max_{\alpha \in X_s} \left| \sum_{a \in H_n} e\left(\frac{\alpha \cdot a}{p}\right) \right| \ll \begin{cases} p^{\frac{n}{2}} & \text{if } s = 0, \\ p^{s-1} & \text{if } 1 \leq s \leq n, \end{cases}$$

where X_s denotes the set of $\alpha \in \mathbb{Z}_p^{n+1}$ with exactly s zero coordinates.

Proof. The bounds for the sum in the case $s = 0$ follow from the well known estimate for multiple Kloosterman sums, which was first proved by Deligne [35]. Clearly for $s = n+1$ (that is $\alpha = (0, \dots, 0)$ the sum counts the number of points in H_n, which is $(p-1)^n$.

For any $1 \leq s \leq n$, let us consider $\alpha \in X_s$. Without loss of generality we can assume that $\alpha_1 = \cdots = \alpha_s = 0$ and $\alpha_i \neq 0$ for $s+1 \leq i \leq n+1$: in particular $\alpha_{n+1} \neq 0$.

Under these asumptions we can rewrite the exponential sum as follows:

$$\sum_{a \in H_n} e\left(\frac{\alpha \cdot a}{p}\right) = \sum_{x_n=1}^{p-1} \cdots \sum_{x_1=1}^{p-1} e\left(\frac{\alpha_{s+1}x_{s+1} + \cdots + \alpha_n x_n + \alpha_{n+1}(x_1 \cdots x_n)^{-1}}{p}\right).$$

Since $\alpha_{n+1} \neq 0$,

$$\sum_{x_1=1}^{p-1} e\left(\frac{\alpha_{n+1}(x_1 \cdots x_n)^{-1}}{p}\right) = -1$$

holds for any choice of $x_1, \dots x_n$, $1 \leq x_i \leq p-1$, and therefore

$$\begin{aligned} \sum_{a \in H_n} e\left(\frac{\alpha \cdot a}{p}\right) &= -(p-1)^{s-1} \prod_{i=s+1}^{n} \sum_{x_i=1}^{p-1} e\left(\frac{\alpha_i x_i}{p}\right) \\ &= (-1)^{n+1-s}(p-1)^{s-1}. \end{aligned}$$

□

We will follow the lines of the proof of Theorem 1 to improve the error term obtained by means of classical techniques in exponential sums.

Theorem 2. *Let p be a prime and H_n be the n-dimensional hyperbola defined in* (1.21)*. For any cube $B \subseteq \mathbb{Z}_p^{n+1}$, of side length M, we have*

$$\left| |H_n \cap B| - \frac{|B|}{p} \right| \ll p^{\frac{n}{2}} \left(1 + \log_+^{n+1}\left(|B|p^{-\frac{n+2}{2}}\right)\right) + \frac{|B|^{1-\frac{1}{n+1}}}{p} \log p.$$

In particular, the asymptotic

$$|H_n \cap B| \sim \frac{|B|}{p}$$

holds as long as $|B|p^{-\frac{n+2}{2}} \to \infty$.

The classical bounds for this problem give

$$|H_n \cap B| = \frac{|B|}{p} + O\left(p^{\frac{n}{2}} \log^{n+1} p + \frac{|B|^{1-\frac{1}{n+1}}}{p} \log p\right),$$

which provides an asymptotic estimate when $|B|p^{-\frac{n+2}{2}}\log^{-n-1}p\to\infty$.

Once again, Theorem 2 improves the classical bounds by extending the range for an asymptotic behaviour: asymptotic estimates hold for any box of size $|B|p^{-\frac{n+2}{2}}\to\infty$.

For $n\geq 4$ Shparlinski [92] obtained a better bound by exploiting multiplicative characters, but in the case $n=2,3$ Theorem 2 is still better that what was known.

Proof of Theorem 2: The proof is analogous to the one from Theorem 1, but considering a partition of all characters depending on the number of zero coordinates of them.

Recall that $B=\prod_{i=1}^{n+1}[H_i+1,H_i+M],\ 1\leq M\leq p$, is a cube in $\mathbb{Z}_p^{n+1}$ of side M. Consider the following approximations of B

$$B'=\prod_{i=1}^{n+1}[H_i+1-m,H_i+M],\quad B''=\prod_{i=1}^{n+1}[H_i+1,H_i+M-m],$$

for some suitable integer $m, 0\leq m\leq M-1$. Denote by $C=\prod_{i=1}^{n+1}[0,m]$.

Then, it is clear that

$$|H_n\cap B|\leq\frac{|B|}{p}+\frac{(|B'|-|B|)}{p}+\frac{1}{p^{n+1}|C|}\sum_{\psi\neq\psi_0}\sum_{H_n,\,B,\,C}\psi(b+c-x),\tag{1.22}$$

$$|H_n\cap B|\geq\frac{|B|}{p}-\frac{(|B|-|B''|)}{p}-\frac{1}{p^{n+1}|C|}\sum_{\psi\neq\psi_0}\sum_{H_n,\,B,\,C}\psi(b+c-x).\tag{1.23}$$

Let us focus on the estimate of (1.22), since the estimate for (1.23) is analogous.

Consider the partition of all non trivial characters indexed by the sets $X_0,\ X_1,\ \ldots,\ X_n$ defined in Proposition 2. Recall that the set X_s consists of all $\alpha\in\mathbb{Z}_p^{n+1}$ with exactly s zero coordinates.

For a fixed character ψ_α, $\alpha\in X_s$, it follows by the bounds given in (1.8) that

$$\left|\sum_C\psi_\alpha(c)\right|=\prod_{i=1}^{n+1}\left(\sum_{c_i=0}^{m}e\left(\frac{\alpha_ic_i}{p}\right)\right)\ll(m+1)^s\prod_{j:\,\alpha_j\neq0}\min\left\{\tfrac{4p}{|\alpha_j|},m+1\right\},$$

and analogously

$$\left|\sum_{B'}\psi_\alpha(b)\right|\ll M^s\prod_{j:\,\alpha_j\neq0}\min\left\{\tfrac{4p}{|\alpha_j|},2M\right\}.$$

Thus, when summing up over all $\alpha\in X_s$ and using the estimates given in (1.9)

$$\sum_{\alpha\in X_s}\left|\sum_C\psi_\alpha(c)\right|\left|\sum_{B'}\psi_\alpha(b)\right|\ll(m+1)^{n+1}M^sp^{n+1-s}\left(1+\log^{n+1-s}\left(\frac{M}{m+1}\right)\right).$$

Taking this into account and partitioning the last sum in (1.22) we have

$$\left||H_n\cap B|-\frac{|B|}{p}\right|\ll\frac{|B|m}{pM}+\sum_{s=0}^{n}|\widehat{H}_{n,s}|\left(\frac{M}{p}\right)^s\left(1+\log^{n+1-s}\left(\frac{M}{m+1}\right)\right).$$

As for Theorem 1, we might choose $m = \min\left\{\left\lfloor M\frac{p^{1+\frac{n}{2}}}{|B|}\right\rfloor, M-1\right\} \leq M-1$ to minimize the error and obtain:

$$\begin{aligned}\left||H_n \cap B| - \frac{|B|}{p}\right| \ll & \sum_{s=0}^{n} |\widehat{H}_{n,s}| \left(\frac{M}{p}\right)^s \left(1+\log_+^{n+1-s}\left(|B|p^{-\frac{n+2}{2}}\right)\right) \\ \ll & p^{\frac{n}{2}}\left(1+\log_+^{n+1}\left(|B|p^{-\frac{n+2}{2}}\right)\right) + \frac{M^n}{p}\left(1+\log_+\left(|B|p^{-\frac{n+2}{2}}\right)\right)\end{aligned}$$

Which concludes the proof by noting that $|B| = M^{n+1}$.

□

1.3 An additive problem in finite fields

Let p be a large prime and g a primitive root modulo p. Andrew Odlyzko asked for which values of M the set

$$g^x - g^y \pmod p \quad 1 \leq x, y \leq M, \tag{1.24}$$

contains every residue class modulo p. He conjectured that one can take M to be as small as $p^{1/2+\epsilon}$, for any fixed $\epsilon > 0$ and p large enough in terms of ϵ.

Observe that the set of differences in (1.24) have at most M^2 elements. Therefore, if true, the conjecture would be essentially the best possible.

Some results have been obtained in this direction. Rudnick and Zaharescu [87], using standard methods of character sums, proved that one can take $M \geq cp^{3/4}\log p$ for some $c > 0$. This range was improved to $M \geq cp^{3/4}$ by Garaev and Kueh [48] and independently by Konyagin [65]. Later, García [49] showed that $c = 2^{5/4}$ is an admissible constant and Cilleruelo [21], using a combinatorial approach, improved the constant to $\sqrt{2}+\varepsilon$, but for p large enough in terms of $\epsilon > 0$.

In this section, we exploit properties of Sidon sets, combined with the classic exponential sums techniques, to obtain new results on a generalization of the original problem of Odlyzko.

We will no longer study differences of powers of primitive roots in prime fields, but differences of elements of large multiplicative order in arbitrary finite fields $\mathbb{F}_q$. Let us write $\mathrm{ord}_q(\theta)$ for the multiplicative order of θ in $\mathbb{F}_q$.

Theorem 3. *Let θ be an element of $\mathbb{F}_q$. If $\min(ord_q(\theta), M) \geq \sqrt{2}q^{3/4}$, then*

$$\{\theta^x - \theta^y : 1 \leq x, y \leq M\} = \mathbb{F}_q.$$

Applying the previous result when θ is a primitive root we obtain the announced improvment on the problem of Odlyzko.

Corollary 6. *Let g be a primitive root of $\mathbb{F}_q$. If $M \geq \sqrt{2}q^{3/4}$, then*

$$\{g^x - g^y : 1 \leq x, y \leq M\} = \mathbb{F}_q.$$

One can generalize Theorem 3, by considering the set of sums of powers of two elements in the field.

Theorem 4. *Let θ_1, θ_2 be two elements of $\mathbb{F}_q$. If*

$$\min(ord_q(\theta_1), \lfloor M_1/2 \rfloor) \cdot \min(ord_q(\theta_2), \lfloor M_2/2 \rfloor) \geq q^{3/2},$$

then

$$\begin{aligned}\mathbb{F}_q^* \subseteq &\{\theta_1^x + \theta_2^y : 1 \leq x \leq M_1,\ 1 \leq y \leq M_2\},\\ \mathbb{F}_q = &\{\theta_1^x - \theta_2^y : 1 \leq x \leq M_1,\ 1 \leq y \leq M_2\}.\end{aligned}$$

Observe that if $\theta_1 = \theta_2 = g$ and $M_1 = M_2 = M$, the condition on M is $M \geq 2q^{3/4}$. The loss on the constant $1/\sqrt{2}$ in the hypothesis relies on the fact that the set $\{\theta_1^x - \theta_2^y : x \leq M_1,\ 1 \leq y \leq M_2\}$ is no longer symmetric if $\theta_1 \neq \theta_2$ or $M_1 \neq M_2$.

Let us recall that that 0 may not belong to the set of sums. Consider for example if θ_1, θ_2 have order $(q-1)/2$, the elements $\theta_1^x + \theta_2^y$ are sum of two squares and 0 do not have a representation of this form if $q = p \equiv 3 \pmod 4$.

We will now prove Theorems 3 and 4 by a direct application of Corollary 1 to appropriate sets B. Let us note that, for the sets

$$A^{\pm}(g_1, g_2, \lambda) = \{(x, y) : g_1^x \pm g_2^y \equiv \lambda \pmod p\}$$

defined before, Corollary 1 implies that if $A \cap B = \emptyset$ then

$$|B| \leq \frac{|\widehat{A}||G|}{|A| + |\widehat{A}|} \leq \frac{q^{1/2}(q-1)^2}{q + q^{1/2} - 2} < q^{3/2} - q + q^{1/2} + 1/2.$$

Proof of Theorem 4: Let us assume that there exists a fixed nonzero element λ of $\mathbb{F}_q$ with no solutions to

$$\theta_1^x + \theta_2^y = \lambda \text{ in } \mathbb{F}_q \text{ with } 1 \leq x \leq M_1,\ 1 \leq y \leq M_2,$$

where

$$\min(\mathrm{ord}_q(\theta_1), \lfloor M_1/2 \rfloor) \cdot \min(\mathrm{ord}_q(\theta_2), \lfloor M_2/2 \rfloor) \geq q^{3/2}. \tag{1.25}$$

Let us denote by $n_1 = \frac{q-1}{\mathrm{ord}_q(\theta_1)}$ and let g_1 be a generator of $\mathbb{F}_q^*$ satisfying $\theta_1 = g_1^{n_1}$. We define n_2 and g_2 analogously. Consider the Sidon set

$$A = A^+(g_1, g_2, \lambda)$$

and the set

$$B = \{(n_1 x, n_2 y) : 1 \leq x \leq \lfloor M_1/2 \rfloor,\ 1 \leq y \leq \lfloor M_2/2 \rfloor\}.$$

It is clear that under the previous assumption above we have that $(B + B) \cap A = \emptyset$. Then we apply Corollary 1 to this case taking into account that

$$|B| = \min(\mathrm{ord}_q(\theta_1), \lfloor M_1/2 \rfloor) \min(\mathrm{ord}_q(\theta_2), \lfloor M_2/2 \rfloor) < q^{3/2} - q + q^{1/2} + 1/2 < q^{3/2}$$

for $q \geq 2$, which contradicts (1.25). The same argument holds for the set of differences by fixing $A = A^-(g_1, g_2, \lambda)$.

□

Proof of Theorem 3: It is clear that the zero element has a representation of the desired form. Let us assume that

$$\min(\mathrm{ord}_q(\theta), M) \geq \sqrt{2}q^{3/4}$$

and that there exists a fixed nonzero element λ of $\mathbb{F}_q$ with no solutions to

$$\theta^x - \theta^y = \lambda \text{ in } \mathbb{F}_q \text{ with } 1 \leq x, y \leq M. \tag{1.26}$$

Let us denote by $n = \frac{q-1}{\mathrm{ord}_q(\theta)}$ and let g be a generator of $\mathbb{F}_q^*$ satisfying $\theta = g^n$. Consider the Sidon set

$$A = A^-(g, g, \lambda)$$

and the set $B = B_1 \cup B_2$ where

$$\begin{aligned} B_1 &= \{(nx, ny) : \ 1 \leq x, y \leq \lfloor M/2 \rfloor, \} \\ B_2 &= B_1 + \left(\tfrac{q-1}{2}, \tfrac{q-1}{2}\right). \end{aligned}$$

We claim that

$$(B + B) \cap A = \emptyset. \tag{1.27}$$

Indeed, any element of $B + B$ is of the form

$$\left(nx + \delta\tfrac{q-1}{2}, ny + \delta\tfrac{q-1}{2}\right),$$

where $\delta \in \{0, 1\}$ and $1 \leq x, y \leq M$. If one of these elements would belong to A, then

$$g^{nx+\delta\frac{q-1}{2}} - g^{ny+\delta\frac{q-1}{2}} = \lambda.$$

Since $g^{\frac{q-1}{2}} = -1$, then either $\theta^x - \theta^y = \lambda$ or $\theta^y - \theta^x = \lambda$ occur in $\mathbb{F}_q$, according to the value of δ. Therefore equation (1.26) would have a solution.

Corollary 1 and (1.27) imply an upper bound for $|B|$:

$$|B| < q^{3/2} - q + q^{1/2} + 1/2. \tag{1.28}$$

We will get now the lower bound:

$$|B| \geq q^{3/2} - \sqrt{2}q^{3/4} + 1/2. \tag{1.29}$$

If $M \geq \mathrm{ord}_q(\theta) = \frac{q-1}{n} > \sqrt{2}q^{3/4}$, then

$$\begin{aligned} \left\{(nx, ny) : \ 1 \leq x, y \leq \tfrac{q-1}{2n}\right\} &\subset B_1, \\ \left\{\left(nx + \tfrac{q-1}{2}, ny + \tfrac{q-1}{2}\right) : \ 1 \leq x, y \leq \tfrac{q-1}{2n}\right\} &\subset B_2. \end{aligned}$$

Since both sets on the left side are disjoint, we have that

$$|B| \geq 2\left\lfloor \tfrac{q-1}{2n} \right\rfloor^2 \geq 2\left\lfloor \tfrac{\mathrm{ord}_q(\theta)}{2} \right\rfloor^2$$

If $M < \mathrm{ord}_q(\theta) = \frac{q-1}{n}$, the sets B_1 and B_2 are disjoint and we have

$$|B| = 2\left\lfloor \tfrac{M}{2} \right\rfloor^2$$

In both cases we have that

$$|B| \geq 2\left\lfloor \frac{\min(\mathrm{ord}_q(\theta), M)}{2} \right\rfloor^2 \geq 2\left(\frac{q^{3/4}}{\sqrt{2}} - \frac{1}{2}\right)^2 = \left(q^{3/4} - 1/\sqrt{2}\right)^2$$
$$= q^{3/2} - \sqrt{2}q^{3/4} + 1/2$$

as we wanted to show.

Next we observe that if (1.28) and (1.29) hold then

$$q < \sqrt{2}q^{3/4} + q^{1/2}.$$

This inequality does not hold for $q \geq 16$ and it proves the theorem for q in this range.

When $q < 16$, we observe that by assumption $\min(\mathrm{ord}_q(\theta), M) \geq \sqrt{2}q^{3/4} > q/2$ (since $q/2 \leq 2q^{3/4}$ implies $q \geq 64$). Suppose that $\lambda \notin D - D$ where $D = \{\theta^x : \ 1 \leq x \leq M\}$ and $|D| = \min(\mathrm{ord}_q(\theta), M) > q/2$. Then $D \cap (D + \lambda) = \emptyset$ and we have that

$$q \geq |D \cup (D + \lambda)| = 2|D| = 2 \cdot \min(\mathrm{ord}_q(\theta), M) > q,$$

which is a contradiction. □

Chapter 2

Concentration: points on curves in small boxes

Studying the distribution of integer and rational points on curves and on algebraic varieties that belong to a given box is a classical topic in analytic number theory. For the case of general plane curves with integer coefficients essentially the best possible results are due to Bombieri and Pila [8, 84, 85]. Furthermore, recently remarkable progress has been made in the case of hypersurfaces and varieties over the rationals (see the surveys [11, 58, 96] as well as the original works [57, 75, 74, 89]).

Significantly less is known about the distribution of points in boxes on curves and varieties in finite fields. As studied in Chapter 1, for reasonably large boxes bounds on exponential sums, that in turn are based on deep methods of algebraic geometry, lead to asymptotic formulas for the number of such points. Certainly when the size of the box is decreasing, then beyond a certain threshold no asymptotic formula is possible (in fact the expected number of points can be less than 1). In particular, for such a small box only one can expect to derive upper bounds on the number of points on curves that hit it. This question was introduced in [22] in the case of the hyperbola and has been intensively studied ever since, having obtained a series of general results.

In the present chapter we will present new ideas and make significant advances in this direction. We obtain upper bounds for the number of solutions to

$$\begin{cases} F(x,y) \equiv 0 \pmod{p} \\ x, y \in B = [R+1, R+M] \times [S+1, S+M], \end{cases}$$

where $F \in \mathbb{F}_p[X,Y]$ denotes either a conic section $Q(x,y)$ or has the form $y^2 - f(x)$ or $y - f(x)$, where $f \in \mathbb{F}_p[X]$ is a polynomial of degree $m \geq 3$.

In Section 2.1 we obtain upper bounds for the cardinality of $|A_Q \cap B|$, where A_Q denotes the set of solutions (x,y) to $Q(x,y) \equiv 0 \pmod{p}$ for some quadratic polynomial Q.

Theorem 5. *Let $Q(x,y)$ be a quadratic polynomial defined over $\mathbb{Z}$, with discriminant $\Delta \neq 0$. For any prime p such that $Q(x,y)$ is absolutely irreducible modulo p and any square box B, we*

have

$$|A_Q \cap B| \ll \left(\frac{|B|^{2+o(1)}}{p}\right)^{1/3} + |B|^{o(1)}.$$

In Section 2.2 we study curves of the form

$$C_f = \{(x, y) : y^2 \equiv f(x) \pmod p, \}$$

for some polynomial $f \in \mathbb{Z}[X]$ and obtained the following results.

Corollary 7. *Uniformly over all polynomials $f \in \mathbb{Z}[X]$ of degree 3 and any square B we have*

$$|C_f \cap B| \le |B|^{1/2+o(1)} \times \begin{cases} |B|^{-2/6} & \text{if } |B| < p^{2/9} \\ \left(\frac{|B|^{5/2}}{p}\right)^{1/6} & \text{if } p^{2/9} \le |B| < p^{1/4} \\ \left(\frac{|B|^{2}}{p}\right)^{1/6} & \text{if } p^{1/4} \le |B| < p^{10/23} \\ \left(\frac{|B|^{3/2}}{p}\right)^{1/16} & \text{if } p^{10/23} \le |B| < p^{2/3} \end{cases}$$

as $|B| \to \infty$.

The above result is a summary of Theorems 6-9 and, unfortunately, does not cover the range $p^{2/3} \le |B| \le p$ in which the only nontrivial upper bound was recently obtained by Chang [15] up to $p^{18/23}$. Observe that, for $|B| \gg p$ bounds obtained in Chapter 1 imply non-trivial bounds in this range, but still nothing is known in the intermediate range $p^{18/23} < |B| \ll p$.

For larger degree polynomials we obtain the following bounds, which depend on $\kappa(m)$, a quantity related to the number of solutions to certain system of Diophantine equations and, by a recent result of Wooley [102], we know that is $m(m-1)/2 \le \kappa(m) \le m^2 - 1$.

Theorem 10. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree $m \ge 3$ and any square B we have*

$$|C_f \cap B| \le |B|^{1/2+o(1)} \left(\frac{|B|^{3/2}}{p}\right)^{1/2\kappa(m)} + |B|^{1/2-(m-3)/4\kappa(m)+o(1)}$$

as $|B| \to \infty$.

In Section 2.3 we study the distribution of polynomial values. For a polynomial $f \in \mathbb{Z}[X]$ we obtain bounds for the number of points in the set

$$A_f = \{(x, y) : y \equiv f(x) \pmod p\}$$

with coordinates in a square B.

Theorem 11. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree $\deg f = m \ge 2$ and any square B we have*

$$|A_f \cap B| \ll \frac{|B|}{p} + |B|^{1/2-1/2^m} p^{o(1)}$$

as $|B| \to \infty$.

Note that in the case of curves modulo p it is not quite clear what one can expect as an "optimal" result (in contrast to the case of estimating integer points in boxes on plane curves

over $\mathbb{Q}$). Yet in some parameter ranges our results are the best possible and can be considered as modulo p analogues of the results of Bombieri and Pila [8, 84, 85].

To complete the discussion, we will also point out further applications of the presented results: we study the distribution of isomorphism classes of hyperelliptic curves of genus $g \geq 1$ in some families of curves associated with polynomials with coefficients in a small box. Surprisingly enough, in the case of the genus $g \geq 2$ we obtain estimates and use methods that do not apply to elliptic curves (that is, to $g = 1$).

We also consider polynomial dynamical systems and study for how long a particular trajectory of such a system can be "locked" in a given box. Extending and improving several results of [13, 14, 23, 54].

Section 2.1 should be considered as a warm up for those sections to come. Most of the proofs discussed in this chapter follow the same spirit as the one presented there, although the methods exploited are clearly deeper and more refined. In fact, they rely on connections between the problem of distribution of points in small boxes on modular curves with some delicate combinations of results from geometry of numbers, Diophantine approximation theory, the Vinogradov mean value theorem and the Weyl method.

The strategy of the proof is based on ideas from Cilleruelo and Garaev [22]. Roughly speaking, we transform the desired congruence to an equivalent congruence keeping control over the coefficients, that will be small compared to p and M. This process can be done by means of simple algebraic transformations or more sophisticated methods. After that, we will lift the problem to the integers and estimate the number of solutions in every of the possible equations arising from the new constructed congruence. To do so, we will need good upper bounds over the number of lattice points in arcs of certain length on conics or more general curves which are described in Appendix A, in Section A.1 and Section A.6.

2.1 Bounds for quadratic polynomials

Let $Q(X, Y) \in \mathbb{Z}[X, Y]$ be a quadratic polynomial with discriminant $\Delta \neq 0$. For any odd prime p, we consider the congruence

$$\begin{cases} Q(x, y) \equiv 0 \pmod{p}, \\ (x, y) \in B = [R + 1, R + M] \times [S + 1, S + M]. \end{cases} \tag{2.1}$$

The objective of this section is to study the number of solutions to (2.1) or, equivalently, the number of points in $A_Q = \{(x, y) \in \mathbb{F}_p^2 : \ Q(x, y) \equiv 0 \pmod{p}\}$ lying in the square B, when this one is qualitatively small with respect to p.

As we have discussed in Chapter 1, it follows from Bombieri's bound that whenever Q is absolutely irreducible we have that

$$|A_Q \cap B| = \frac{|B|}{p} + O\left(p^{1/2} \log_+^2\left(|B|p^{-3/2}\right)\right).$$

The previous bound provides us a non-trivial upper bound for the number of points in $A_Q \cap B$ as long a B is sufficiently large: that is, for $|B| \geq p$. Nevertheless, beyond this threshold

results based on exponential and character sums turn out to be insufficient and new methods and techniques are required to obtain any non-trivial upper bound for the quantity $|A_Q \cap B|$.

Let us now state the main result of this section.

Theorem 5. *Let $Q(x, y)$ be a quadratic polynomial defined over $\mathbb{Z}$, with discriminant $\Delta \neq 0$. For any prime p such that $Q(x, y) \pmod p$ is absolutely irreducible of degree 2 and any square box B, we have*

$$|A_Q \cap B| \ll |B|^{o(1)} \left(\frac{|B|^2}{p}\right)^{1/3} + |B|^{o(1)}.$$

This estimate is not trivial when $|B| = o(p^2)$ and better than the classical bounds, whenever $|B| \ll p^{5/4}$. Furthermore, when $|B| \ll p^{1/2}$ Theorem 5 gives $|A_Q \cap B| = |B|^{o(1)}$, which is sharp.

Note that if Q is reducible modulo p, namely

$$Q(x, y) \equiv q_1(x, y)q_2(x, y) \pmod p,$$

for some linear polynomials $q_i(x, y) \in \mathbb{Z}[x, y]$, solutions in (2.1) will correspond to solutions of any of the linear equation $q_i(x, y) \equiv 0 \pmod p$ and we could have $\gg |B|^{1/2}$ different solutions. The condition of irreducibility is required to avoid this situation.

Observe that the condition $\Delta \neq 0$ restrict ourselves to the study of ellipses and hyperbolas. The given upper bound cannot be applied to quadratic polynomials with discriminant $\Delta = 0$. For example the number of solutions to (2.1) when $Q(x, y) = y - x^2$ is $\asymp |B|^{1/4}$ (which is still absolutely irreducible over any field).

Proof of Theorem 5. Let $Q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$ be a quadratic polynomial with integer coefficients and discriminant $D = b^2 - 4ac \neq 0$. Whenever $a = c = 0$, the congruence in (2.1) can be written in the form $XY \equiv \mu \pmod p$, where $X = bx + e$, $Y = by + d$ and $\mu = b\lambda - (ed + bf)$. This case was already studied in [22], but one extra condition was required: μ must be coprime with p or, equivalently, $XY - \mu$ must be absolutely irreducible modulo p.

If $a \neq 0$ the congruence in (2.1) can be written as

$$X^2 - DY^2 \equiv \mu \pmod p,$$

where $X = Dy + 2(ae - db)$, $Y = 2ax + by + d$ and $\mu = 4aD\lambda - D(4af - d^2) + 4a(ae - db)$. The case $a = 0$ and $c \neq 0$ follows by exchanging x for y in the previous argument (and so c, e will be the coefficients of x^2 and x instead of a, d). Our new variables X, Y lie in intervals of length $\ll M$. Specifically X lies in an interval of length DM and Y in an interval of length $(2|a| + |b|)M$.

We also can assume that $p > D$. Since $D \neq 0$, different original solutions will lead us to a different solution.

These observations allow us to bound the number of solutions to (2.1) by the number of solutions of the congruence

$$x^2 - Dy^2 \equiv \mu \pmod p,$$

where x, y lie in two intervals of length $\ll M$.

Without loss of generality we can assume that D is square-free. Otherwise $D = D_1 k^2$, for some square-free integer D_1, and solutions (x, y) of our equation would lead us to solutions (x, ky) of $x^2 - D_1(ky)^2 \equiv \mu \pmod p$, where ky would lie in some interval of length $\ll M$. The case $D = 1$ corresponds to the problem $x^2 - y^2 = UV \equiv \mu \pmod p$, where $U = (x + y)$ and $V = (x - y)$ still lie in some intervals of length $\ll M$ and $(\mu, p) = 1$, otherwise $UV - \mu$ will be reducible modulo p. Once more this case was already studied in [22].

By the previous arguments it is enough to prove the result for

$$x^2 - Dy^2 \equiv \lambda \pmod p, \qquad \begin{cases} R + 1 \leq x \leq R + M, \\ S + 1 \leq y \leq S + M, \end{cases} \tag{2.2}$$

where D is some square-free integer $\neq 0, 1$ and $\lambda \in \mathbb{Z}$.

This equation is equivalent to

$$\left(x^2 + 2Rx\right) - D\left(y^2 + 2Sy\right) \equiv \mu \pmod p, \qquad 1 \leq x, y \leq M,$$

where $\mu = \lambda - (R^2 - DS^2)$. By the pigeonhole principle we have that for every positive integer $T < p$, there exists a positive integer $t < T^2$ such that $tR \equiv r_0 \pmod p$ and $tS \equiv s_0 \pmod p$ with $|r_0|, |s_0| < p/T$. Thus we can always rewrite the equation (2.2) as

$$\left(tx^2 + 2r_0x\right) - D\left(ty^2 + 2s_0y\right) \equiv \mu_0 \pmod p, \qquad 1 \leq x, y \leq M,$$

where $|\mu_0| < p/2$. This modular equation lead us to the following Diophantine equation

$$\left(tx^2 + 2r_0x\right) - D\left(ty^2 + 2s_0y\right) = \mu_0 + pz, \qquad 1 \leq x, y \leq M,\ z \in \mathbb{Z}, \tag{2.3}$$

where z must satisfy

$$|z| = \left| \frac{\left(tx^2 + 2r_0x\right) - D\left(ty^2 + 2s_0y\right) - \mu_0}{p} \right| < \frac{(1 + |D|)T^2M^2}{p} + \frac{2(1 + |D|)M}{T} + \frac{1}{2}.$$

For each integer z on the previous range the equation defined in (2.3) is equivalent to:

$$(tx + r_0)^2 - D(ty + s_0)^2 = n_z, \qquad 1 \leq x, y \leq M, \tag{2.4}$$

where $n_z = t(\mu_0 + pz) + (r_0^2 - Ds_0^2)$. We will now study the number of solutions in terms of n_z.

If $n_z = 0$, since D is not a square, we have that $tx + r_0 = ty + s_0 = 0$ and there is at most one solution (x, y).

Let now focus on the case $n_z \neq 0$. We will split the problem in two different cases, depending on how big M is compared to p.

- Case $M < \frac{p^{1/4}}{4\sqrt[4]{(1+|D|)^3}}$. In this case we take $T = 8\,(1 + |D|)\,M$ in order to get $|z| < 1$. Therefore it suffices to study solutions of

$$(tx + r_0)^2 - D(ty + s_0)^2 = n_0, \qquad 1 \leq x, y \leq M.$$

  If $n_0 > 2^{48}(1 + |D|)^{12}M^{18}$, the integers $|tx + r_0|$ and $|ty + s_0|$ will lie in two intervals of length $T^2M = 2^6(1 + |D|)^2M^3$ and solutions to (2.2) will come from lattice points in an

arc of length smaller than $2^8(1+|D|)^2M^3 < n_0^{1/6}$ (by hypothesis). From Lemma 15 it follows that there will be no more than two lattice points in such an arc.

If $n_0 \leq 2^{48}(1+|D|)^{12}M^{18}$, Lemma 16 assures that the number of solutions will be $M^{o(1)}$.

- Case $M \geq \frac{p^{1/4}}{4\sqrt[4]{(1+|D|)^3}}$. In this case we take $T = (p/M)^{1/3}$ and hence $|z| \ll \frac{M^{4/3}}{p^{1/3}}$. Since $n_z = t(\mu_0 + pz) + (r_0^2 - Ds_0^2) \ll p^2 \ll M^8$ we can apply Lemma 16 to conclude that for every z in the above range there will be $M^{o(1)}$ solutions to its related Diophantine equation.

We have proved that in all cases, the number of solutions to (2.4) is $M^{o(1)}$ for each n_z. On the other hand, the number of possible values of z is $O(M^{4/3}p^{-1/3}+1)$. It follows that

$$|A_Q \cap B| \ll \left(M^{4/3}p^{-1/3}+1\right) M^{o(1)} = \left(\left(|B|^2/p\right)^{1/3}+1\right)|B|^{o(1)}.$$

□

2.2 Points on curves in small boxes

In this section we will study those curves of the form:

$$C_f = \{(x,y) :\ y^2 \equiv f(x) \pmod p\} \subseteq \mathbb{F}_p \times \mathbb{F}_p$$

and obtain bounds for the quantity $|C_f \cap B|$ uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of fixed degree m.

Note that, for all such curves, the trivial upper bound for the number of points with coordinates in a given squared box $B = [R+1, R+M] \times [S+1, S+M]$ is precisely $2|B|^{1/2}$, since for any given $R+1 \leq x \leq R+M$ there are at most two solutions to the congruence $f(x) \equiv Y^2 \pmod p$. Therefore, our goal is to obtain bounds at least $o\left(|B|^{1/2}\right)$ for this type of curves.

2.2.1 Polynomials of degree 3

When the degree of f is $m = 3$ it is clear that for any $f \in \mathbb{F}_p[X]$ the curve $f(X) \equiv Y^2 \pmod p$ is absolutely irreducible modulo p. In this case, general bounds on the number of points on a curve in a given box, see Theorem 1, imply that

$$|C_f \cap B| = \frac{|B|}{p} + O\left(p^{1/2}\log_+^2\left(|B|p^{-3/2}\right)\right). \tag{2.5}$$

Note that this estimate implies

$$|C_f \cap B| \ll \begin{cases} p^{1/2} & \text{if } p \leq |B| < p^{3/2}, \\ |B|/p & \text{if } p^{3/2} \leq |B| < p^2, \end{cases}$$

but note that (2.5) is worse than the trivial upper bound when $|B| \ll p^{1/2}$.

Corollary 7. *Uniformly over all polynomials $f \in \mathbb{Z}[X]$ of degree 3, and any square B we have*

$$|C_f \cap B| \le |B|^{1/2+o(1)} \times \begin{cases} |B|^{-2/6} & \text{if } |B| < p^{2/9} \quad \text{(Theorem 6)} \\ \left(\frac{|B|^{5/2}}{p}\right)^{1/6} & \text{if } p^{2/9} \le |B| < p^{1/4} \quad \text{(Theorem 7)} \\ \left(\frac{|B|^{2}}{p}\right)^{1/6} & \text{if } p^{1/4} \le |B| < p^{10/23} \quad \text{(Theorem 8)} \\ \left(\frac{|B|^{3/2}}{p}\right)^{1/16} & \text{if } p^{10/23} \le |B| < p^{2/3} \quad \text{(Theorem 9)} \end{cases}$$

as $|B| \to \infty$.

In the range $p^{2/3} \le |B| < p$ no upper bounds are known rather than the trivial one.

Recall that if $|B| < p^{2/9}$ not only we have a non-trivial bound, but we showed that the number of solutions is $\ll |B|^{1/6+o(1)}$ which is sharp up to the $o(1)$ constant.

Theorem 6. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree 3 and any square B, with $1 \le |B| \le p^{2/9}$, we have*

$$|C_f \cap B| \le |B|^{1/6+o(1)}$$

as $|B| \to \infty$.

Let us recall that no upper bound better than $|B|^{1/6}$ is possible. This question will be discussed in Section 2.4.

Proof. Denote the square $B = [R+1, R+M] \times [S+1, S+M]$. We have to estimate the number of solutions to

$$f(R+x) \equiv (S+y)^2 \pmod p,$$

with $1 \le x, y \le M$, which is equivalent to the congruence

$$a_1x^3 + a_2x^2 + a_3x + 1_4y^2 + a_5y \equiv b \pmod p, \tag{2.6}$$

where $(a_1, p) = 1$. Witout loss of generality we can assume $a_1 = 1$.

For any $T \le p^{1/4}/M^{1/2}$, we can apply Lemma 24 to (2.6) with

$$T_1 = T^4M^2, \qquad T_2 = T_4 = p/(TM), \qquad T_3 = T_5 = p/T,$$

and conclude that there exits $|t| \le T^4M^2$ such that

$$\|a_2t\|_p,\ \|a_4t\|_p \le p/(TM), \quad \|a_3t\|_p,\ \|a_5t\|_p \le p/T.$$

Thus, by multiplying both sides of the congruence (2.6) by t, we can replace the congruence (2.6) with the following equation over $\mathbb{Z}$:

$$A_1x^3 + A_2x^2 + A_3x + A_4y^2 + A_5y + A_6 = pz, \tag{2.7}$$

where

$$|A_1| \le T^4M^2, \quad |A_2|, |A_4| \le p/(TM), \quad |A_3|, |A_5| \le p/T, \quad |A_6| \le p/2.$$

Since, for $0 \le x, y \le M$ the left hand side of the equation (2.7) is bounded by $T^4M^5 + 4pM/T + p/2$, it follows that

$$|z| \ll \frac{T^4M^5}{p} + \frac{4M}{T} + 1.$$

The choice $T \sim p^{1/5}/M^{4/5}$ leads us to the bound

$$|z| \ll M^{9/5}p^{-1/5} + 1 \ll 1$$

since $M \le p^{1/9}$.

We note that the polynomial $A_1X^3 + A_2X^2 + A_3X + A_4Y^2 + A_5Y + A_6$ on left hand side of (2.7) is absolutely irreducible. Indeed, it is obtained from $f(X) - Y^2$ (which is an absolutely irreducible polynomial) by a non-trivial modulo p affine transformation. Therefore, for every integer z, the polynomial $A_1X^3 + A_2X^2 + A_3X + A_4Y^2 + A_5Y + A_6 - pz$ is also absolutely irreducible (as its reduction modulo p is absolutely irreducible modulo p).

Thus, for each z in the previous range, equation (2.7) corresponds to an absolutely irreducible curve of degree 3 which, by Lemma 17, has at most $M^{1/3+o(1)}$ points lying in $[0, M]^2$. Therefore, the number of solutions in the original equation is bounded by $M^{1/3+o(1)}$ and the result follows. □

Clearly the argument used in the proof of Theorem 6 works for large values of $|B|$. In particular, for $M > p^{1/9}$, it leads to the bound $|C_f \cap B| \ll M^{32/15+o(1)}p^{-1/5}$ which is non-trivial for $M \le p^{3/17}$.

However, using a modification of this argument we can obtain a stronger bound which is non-trivial for $p^{1/9} < M \le p^{1/5}$.

Theorem 7. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree 3 and any square B, with $p^{2/9} < |B| \le p^{2/5}$, we have*

$$|C_f \cap B| \le |B|^{1/2+o(1)} \left(\frac{|B|^{5/2}}{p}\right)^{1/6}$$

as $|B| \to \infty$.

Proof. Once again denote the square $B = [R+1, R+M] \times [S+1, S+M]$. Let $K = \lfloor p^{1/6}/M^{1/2} \rfloor$ and observe that we have $1 \le K \le M$ when $p^{1/9} < M$. Also observe that one could cover B with $J = O(M/K)$ rectangles of the form $[R_j + 1, R_j + K] \times [S + 1, S + M]$, $j = 1, \dots, J$. Then, the equation in each rectangle can be written as

$$f(x + R_j)\lambda \equiv (y = S)^2 \pmod p \tag{2.8}$$

with $1 \le x \le K$ and $1 \le y \le M$.

To estimate the number of solutions to (2.8), we set

$$T_1 = p^{1/2}M^{3/2}, \quad T_2 = p^{2/3}M, \quad T_3 = p^{5/6}M^{1/2}, \quad T_4 = p/M^2, \quad T_5 = p/M.$$

and apply, once more, Lemma 24 where a_i are the coefficients of x, y in (2.8). Hence, as in the proof of Lemma 6, we obtain an equivalent equation over $\mathbb{Z}$:

$$A_1x^3 + A_2x^2 + A_3x + A_4y^2 + A_5y + A_6 = pz, \tag{2.9}$$

where $|A_i| \le T_i$ for $i = 1, \dots, 5$ and $|A_6| \le p/2$. The left hand side of (2.9) is bounded by

$$\begin{aligned}
&|A_1K^3 + A_2K^2 + A_3K + A_4M^2 + A_5M + A_6| \\
&\quad \le p^{1/2}M^{3/2}\left(\frac{p^{1/6}}{M^{1/2}}\right)^3 + p^{2/3}M\left(\frac{p^{1/6}}{M^{1/2}}\right)^2 + p^{5/6}M^{1/2}\frac{p^{1/6}}{M^{1/2}} + \frac{p}{M^2}M^2 + \frac{p}{M^2}M + p/2 \\
&\quad = 5.5p.
\end{aligned}$$

Thus, z can take at most 11 values. As we have seen in the proof of Theorem 6, the polynomial on the left hand side of (2.9) is absolutely irreducible. Therefore, Lemma 17 implies that, for each value of z, equation (2.9) has at most $M^{1/3+o(1)}$ solutions. Summing over all rectangles we finally obtain that the original congruence has at most

$$(M/K)M^{1/3+o(1)} = M^{11/6+o(1)}p^{-1/6} = M^{1+o(1)}\left(M^5/p\right)^{1/6}$$

solutions. □

A different argument allow us to obtain a better bound for slightly bigger boxes.

Theorem 8. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree 3 and any square B we have*

$$|C_f \cap B| \le |B|^{1/6+o(1)} + \frac{M^{5/6+o(1)}}{p^{1/6}},$$

as $|B| \to \infty$.

Proof. As done before, let us denote the square $B = [R+1, R+M] \times [S+1, S+M]$. For the sake of brevity, we denote $I = |C_f \cap B|$. We can assume that I is large and fix some integer L with

$$1 \le L \le 0.01I, \tag{2.10}$$

to be chosen later. By the pigeonhole principle, there exists Q such that the congruence

$$\begin{cases} y^2 \equiv f(x) \pmod p, \\ Q+1 \le x \le Q + M/L,\ S+1 \le y \le S+M, \end{cases} \tag{2.11}$$

has at least I/L solutions. Let us now estimate the number of solutions to (2.11) to derive bounds for I, for suitable choice of L.

We can split the interval $[Q+1, Q+M/L]$ into $k_0 = \lceil I/(30L) \rceil$ intervals of length not greater than $30M/I$. Since there are at most two solutions to the above congruence with the same value of x, and since we have at least $I/L > 20k_0$ solutions in total, from the pigeonhole principle it follows that there exists an interval of length $30M/I$ containing at least 10 pairwise distinct values of x (corresponding to 10 different solutions (x, y)). Let x_0 be the first of these values and let (x_0, y_0) be the corresponding solution. It is clear that I/L is bounded by the number of solutions of

$$\begin{cases} (y_0+y)^2 \equiv f(x_0+x) \pmod p, \\ -M/L \le x \le M/L, \quad -M \le y \le M, \end{cases}$$

which is equivalent to

$$\begin{cases} y^2 \equiv c_3x^3 + c_2x^2 + c_1x + c_0y \pmod p, \\ -M/L \le x \le M/L, \quad -M \le y \le M, \end{cases} \tag{2.12}$$

with $(c_3, p) = 1$. Besides, there are at least 10 solutions (x, y) with x pairwise distinct and such that $0 \le x \le 30M/I$. From these 10 values we fix 3 solutions $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ and rewrite the congruence (2.12) in the matrix form

$$\begin{pmatrix} x^3 & x^2 & x & y \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod p. \tag{2.13}$$

By Lemma 25, we know that at most 6 pairs (x, y), with x pairwise distinct, satisfy both the congruence (2.13) and the congruence

$$\begin{vmatrix} x^3 & x^2 & x & y \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{vmatrix} \equiv 0 \pmod p.$$

Since there are at least 10 solutions to (2.13), for one of them, say (x_4, y_4), we have

$$\Delta = \begin{vmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{vmatrix} \not\equiv 0 \pmod p.$$

Note that $1 \le |\Delta| \ll (M/I)^6 M$. Now we solve the system of congruences

$$\begin{pmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_4^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod p$$

with respect to (c_3, c_2, c_1, c_0). We write Δ_j for the determinant of the matrix on the left hand side where we have substituted the jth-column by the vector $(y_4^2, y_3^2, y_2^2, y_1^2)$. With this notation we have that

$$c_j \equiv \Delta_{4-j}\Delta^* \pmod p, \quad j = 0, \dots, 3,$$

where Δ^* is defined by $\Delta\Delta^* \equiv 1 \pmod p$, and the congruence (2.12) is equivalent to

$$\Delta_1x^3 + \Delta_2x^2 + \Delta_3x + \Delta_4y - \Delta y^2 \equiv 0 \pmod p.$$

In particular, since, as we have noticed, $c_3 \not\equiv 0 \pmod p$, we have that $\Delta_1 \not\equiv 0 \pmod p$. We can write this congruence as an equation over $\mathbb{Z}$:

$$\Delta_1x^3 + \Delta_2x^2 + \Delta_3x + \Delta_4y - \Delta y^2 = pz, \qquad (x, y, z) \in \mathbb{Z}^3. \tag{2.14}$$

We can easily check that

$$|\Delta_4| \ll (M/I)^6 M^2$$

and

$$|\Delta_j| \ll (M/I)^{2+j} M^3, \qquad j = 1, 2, 3.$$

Thus, collecting the above estimates and taking into account $L \ll I$, we derive

$$\begin{aligned} |z| &\ll \frac{1}{p}\left(|\Delta_1|(M/L)^3 + |\Delta_2|(M/L)^2 + |\Delta_3|(M/L) + |\Delta_4|M + |\Delta|M^2\right) \\ &\ll \frac{M^3}{p}\left(\frac{M^6}{I^3L^3} + \frac{M^6}{I^4L^2} + \frac{M^6}{I^5L} + \frac{M^6}{I^6}\right) \ll \frac{M^9}{pI^3L^3}. \end{aligned}$$

Since $\Delta_1 \neq 0$, $\Delta \neq 0$, for each z, the curve (2.14) is absolutely irreducible, and thus by Lemma 17 it contains at most $M^{1/3+o(1)}$ integer points (x, y) with $|x|, |y| \leq M$. Hence

$$\frac{I}{L} \leq M^{1/3+o(1)}\left(1 + \frac{M^9}{pI^3L^3}\right)$$

for any L satisfying (2.10). This implies, that

$$I \leq LM^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}L^{1/2}}. \tag{2.15}$$

If $M < 10p^{1/8}$, then we take $L = 1$ and derive from (2.15) that

$$I \leq M^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}} \leq M^{1/3+o(1)}.$$

Let now consider the case $M > 10p^{1/8}$. We can assume that $I > M^{5/3}p^{-1/6}$, as otherwise there is nothing to prove. Then we take $L = \left\lfloor M^{4/3}p^{-1/6} \right\rfloor$ and note that the condition (2.10) is satisfied. Thus, we derive from (2.15) that

$$I \leq LM^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}L^{1/2}} \leq M^{5/3+o(1)}p^{-1/6}$$

and the result follows. □

We exploit recent results from Wooley [101] and a result on geometry of numbers, based on ideas from [10], to obtain good estimates for larger values of M, but unfortunately still far from the natural threshold $p^{1/2}$.

Theorem 9. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree 3 and any square B we have*

$$|C_f \cap B| \leq |B|^{1/6+o(1)} + \left(\frac{|B|^{3/2}}{p}\right)^{1/16} |B|^{1/2+o(1)}.$$

Proof. Denote the square $B = [R+1, R+M] \times [S+1, S+M]$. Clearly we can assume that

$$M > p^{5/23} \tag{2.16}$$

as otherwise

$$(M^3/p)^{1/16}M \ge \frac{M^{5/3+o(1)}}{p^{1/6}}$$

and the result follows from Theorem 8. We can also assume that M is sufficiently large and $M = o(p^{1/3})$.

We fix one point $(x_0, y_0) \in C_f$ and by making the change of variables $(x, y) \mapsto (x-x_0, y-y_0)$, we see that it is enough to study a congruence of the form

$$\begin{cases} y^2 - c_0 y \equiv c_3x^3 + c_2x^2 + c_1x \pmod p, \\ |x|, |y| \le M. \end{cases} \tag{2.17}$$

Let $\mathcal{W}$ be the set of pairs (x, y) that satisfy (2.17) and $\mathcal{X}$ denote the set of x for which $(x, y) \in \mathcal{W}$ for some y. Let

$$\rho = \frac{\#\mathcal{X}}{M}.$$

We now fix some $\varepsilon > 0$ and assume that

$$\rho \ge (M^3/p)^{1/16}M^{\varepsilon}. \tag{2.18}$$

In view of (2.16) and (2.18), we also have

$$\rho > M^{-1/10}. \tag{2.19}$$

For $\vartheta > 0$ we define the intervals

$$I_{\nu,\vartheta} = [-\vartheta M^{\nu}, \vartheta M^{\nu}], \qquad \nu = 1, 2, 3,$$

which we treat as intervals in $\mathbb{F}_p$, that is, sets of residues modulo p of several consecutive integers.

We now consider the set

$$\mathcal{S} \subseteq I_{1,8} \times I_{2,8} \times I_{3,8}$$

of all triples

$$\mathbf{s} \equiv (x_1 + \ldots + x_8,\, x_1^2 + \ldots + x_8^2,\, x_1^3 + \ldots + x_8^3) \pmod p, \tag{2.20}$$

where x_i, $i = 1, \ldots, 8$, independently run through the set $\mathcal{X}$. Since $M = o(p^{1/3})$, the congruence

$$\begin{cases} x_1^j + \ldots + x_8^j \equiv x_9^j + \ldots + x_{16}^j \pmod p, \qquad j = 1, 2, 3, \\ |x_i|, |y_i| \le M \end{cases} \tag{2.21}$$

can be lifted to $\mathbb{Z}$, converted to the system of Diophantine equations

$$x_1^j + \ldots + x_8^j = x_9^j + \ldots + x_{16}^j, \quad j = 1, 2, 3,$$

which by Lemma 18 has at most $M^{10+o(1)}$ solutions in integers x_i with $|x_i| \le M$, $i = 1, \ldots, 16$. Therefore, the congruence (2.21) has at most $M^{10+o(1)}$ solutions in $x_i \in \mathcal{X}$, $i = 1, \ldots, 16$, as well. Thus, collecting elements of the set $\mathcal{X}^8$ that correspond to the same vector $\mathbf{s}$ given

by (2.20) and denoting the number of such representations by $N(\mathbf{s})$, if follows from the Cauchy inequality that

$$(\#\mathcal{X})^8 = \sum_{\mathbf{s}\in\mathcal{S}} N(\mathbf{s}) \le \left(\#\mathcal{S}\sum_{\mathbf{s}\in\mathcal{S}} N(\mathbf{s})^2\right)^{1/2} \le \left(\#\mathcal{S}M^{10+o(1)}\right)^{1/2}.$$

Thus

$$\#\mathcal{S} \ge \frac{(\#\mathcal{X})^{16}}{M^{10+o(1)}} = \rho^{16}M^{6+o(1)}.$$

Hence, there exist at least $\rho^{16}M^{6+o(1)}$ triples

$$(z_1, z_2, z_3) \in I_{1,8} \times I_{2,8} \times I_{3,8}$$

such that

$$c_3z_3 + c_2z_2 + c_1z_1 \equiv \widetilde{z}_2 - c_0\widetilde{z}_1 \pmod p$$

for some $\widetilde{z}_2 \in I_{2,8}$ and $\widetilde{z}_1 \in I_{1,8}$. In particular we have that the congruence

$$\begin{cases} c_3z_3 + c_2z_2 + \widetilde{z}_2 + c_1z_1 + c_0\widetilde{z}_1 \equiv 0 \pmod p, \\ (z_1, \widetilde{z}_1, z_2, \widetilde{z}_2, z_3) \in I_{1,8} \times I_{1,8} \times I_{2,8} \times I_{2,8} \times I_{3,8}, \end{cases}$$

has a set of solutions $\mathcal{S}$ with

$$\#\mathcal{S} \ge \rho^{16}M^{6+o(1)}. \tag{2.22}$$

The rest of the proof is based on the ideas from [10]. We define the lattice

$$\Gamma = \{(X_2, X_3, \widetilde{X}_2, X_1, \widetilde{X}_1) \in \mathbb{Z}^5 \ : \\ X_2 + c_3X_3 + c_2\widetilde{X}_2 + c_1X_1 + c_0\widetilde{X}_1 \equiv 0 \pmod p\}$$

and the body

$$D = \{(x_2, x_3, \widetilde{x}_2, x_1, \widetilde{x}_1) \in \mathbb{R}^5 \ : \\ |x_1|, |\widetilde{x}_1| \le 8M,\ |x_2|, |\widetilde{x}_2| \le 8M^2,\ |x_3| \le 8M^3\}.$$

From (2.22), it follows that

$$\#\left(D \cap \Gamma\right) \ge \rho^{16}M^{6+o(1)}.$$

Therefore, by Corollary 18, the successive minima $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1, \dots, 5$, must satisfy the inequality

$$\prod_{i=1}^{5} \min\{1, \lambda_i\} \ll \rho^{-16}M^{-6+o(1)}. \tag{2.23}$$

From the definition of λ_i it follows that there are five linearly independent vectors

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \widetilde{v}_{2,i}, v_{1,i}, \widetilde{v}_{1,i}) \in \lambda_i D \cap \Gamma, \quad i = 1, \dots, 5. \tag{2.24}$$

Indeed, first we choose a nonzero vector $\mathbf{v}_1 \in \lambda_1 D \cap \Gamma$. Then assuming that for $1 \le i \le 5$ the vectors $\mathbf{v}_1, \dots, \mathbf{v}_{i-1}$ are chosen, we choose $\mathbf{v}_i$ as one of the vectors $\mathbf{v} \in \lambda_i D \cap \Gamma$ that are not in the linear space generated by $\mathbf{v}_1, \dots, \mathbf{v}_{i-1}$.

We claim that $\lambda_3 < 1$ and that $\lambda_5 > 1$ (which in particular implies that $\lambda_1, \lambda_2 < 1$ by definition of the λ_i).

To prove the inequality in λ_3, observe that in case $\lambda_3 \geq 1$ from (2.23) we obtain

$$\min\{1, \lambda_1^2\} \leq \min\{1, \lambda_1\} \min\{1, \lambda_2\} \leq \rho^{-16} M^{-6+o(1)}.$$

Thus recalling (2.19) we see that

$$\lambda_1 \leq \frac{1}{10M^2}$$

and the vector $\mathbf{v}_1$ must have $v_{2,1} = \widetilde{v}_{2,1} = v_{1,1} = \widetilde{v}_{1,1} = 0$. In turn this implies that $v_{3,1} \equiv 0 \pmod p$ and since we assumed that $M = o(p^{1/3})$, we obtain $v_{3,1} = 0$, which contradicts the condition that $\mathbf{v}_1$ is a nonzero vector.

To show the second inequality, note that if $\lambda_5 < 1$ by (2.23) we have

$$\prod_{i=1}^{5} \lambda_i \leq \rho^{-16} M^{-6+o(1)}.$$

We now consider the determinant Δ of the 5×5 matrix that is formed by the vectors (2.24). It follows that

$$\Delta \ll M^{2+3+2+1+1} \prod_{i=1}^{5} \lambda_i \leq \rho^{-16} M^{3+o(1)},$$

which, by our assumption (2.18), implies that $|\Delta| < p$. On the other hand, since $\mathbf{v}_i \in \Gamma$, we have $\Delta \equiv 0 \pmod p$, thus $\Delta = 0$ provided that p is large enough, which contradicts the linear independence of the vectors in (2.24).

We now consider separately the following two cases, depending on whether $\lambda_4 \leq 1$ or not.

Case 1: $\lambda_4 \leq 1$. Let

$$\mathbf{V} = \begin{pmatrix} v_{3,1} & \widetilde{v}_{2,1} & v_{1,1} & \widetilde{v}_{1,1} \\ v_{3,2} & \widetilde{v}_{2,2} & v_{1,2} & \widetilde{v}_{1,2} \\ v_{3,3} & \widetilde{v}_{2,3} & v_{1,3} & \widetilde{v}_{1,3} \\ v_{3,4} & \widetilde{v}_{2,4} & v_{1,4} & \widetilde{v}_{1,4} \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} -v_{2,1} \\ -v_{2,2} \\ -v_{2,3} \\ -v_{2,4} \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix}.$$

We have

$$V\mathbf{c} \equiv \mathbf{w} \pmod p.$$

Let

$$\Delta = \det V$$

and let Δ_j be the determinant of the matrix obtained by replacing the j-th column of V by $\mathbf{w}$, $j = 1, \dots, 4$.

Recalling (2.23), we have

$$|\Delta| \ll \lambda_1\lambda_2\lambda_3\lambda_4 M^{3+2+1+1} \leq \rho^{-16} M^{1+o(1)} \tag{2.25}$$

and similarly

$$\begin{aligned} &|\Delta_1| \leq \rho^{-16} M^{o(1)}, \qquad |\Delta_2| \leq \rho^{-16} M^{1+o(1)}, \\ &|\Delta_3| \leq \rho^{-16} M^{2+o(1)}, \qquad |\Delta_4| \leq \rho^{-16} M^{2+o(1)}. \end{aligned} \tag{2.26}$$

Note that, in view of (2.18), in particular we have

$$|\Delta|, |\Delta_j| < p, \quad j = 1, \dots, 4.$$

If $\Delta \equiv 0 \pmod p$ then since $\mathbf{c}$ is nonzero modulo p we also have $\Delta_j \equiv 0 \pmod p$, $j = 1, \dots, 4$, implying that $\Delta = \Delta_j = 0$ (in fact this holds regardless whether $\mathbf{c}$ is zero or not modulo p) Then the matrix formed by $\mathbf{v}_1, \dots, \mathbf{v}_4$ is of rank at most 3, which contradicts their linear independence. Therefore $\Delta \not\equiv 0 \pmod p$ and thus we have

$$c_i \equiv \frac{\Delta_{4-i}}{\Delta} \pmod p, \qquad i = 0, 1, 2, 3.$$

Since $c_3 \not\equiv 0 \pmod p$, we have $\Delta_1 \neq 0$. We now substitute this in (2.17) and get that

$$\Delta y^2 - \Delta_4 y \equiv \Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x \pmod p, \quad |x|, |y| \le M.$$

We see from (2.18), (2.25) and (2.26) that for sufficiently large M the absolute values of the expressions on both sides are less than $p/2$, implying the equality

$$\begin{cases} \Delta y^2 - \Delta_4 y = \Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x, \\ |x|, |y| \le M, \end{cases}$$

over $\mathbb{Z}$. Now we use Lemma 17 and conclude that the number of solutions is at most $M^{1/3+o(1)}$.

Case 2: $\lambda_4 > 1$. We claim that, in this case, $\lambda_3 > (10M)^{-1}$. By (2.23), we have

$$\prod_{i=1}^{3} \lambda_i \le \rho^{-16} M^{-6+o(1)}.$$

Provided $\lambda_3 \le (10M)^{-1}$, we also have

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \widetilde{v}_{2,i}, 0, 0), \quad i = 1, 2, 3. \tag{2.27}$$

In particular,

$$\begin{pmatrix} v_{2,1} & v_{3,1} & \widetilde{v}_{2,1} \\ v_{2,2} & v_{3,2} & \widetilde{v}_{2,2} \\ v_{2,3} & v_{3,3} & \widetilde{v}_{2,3} \end{pmatrix} \begin{pmatrix} 1 \\ c_3 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \pmod p.$$

Thus, for the determinant

$$\Delta = \det \begin{pmatrix} v_{2,1} & v_{3,1} & \widetilde{v}_{2,1} \\ v_{2,2} & v_{3,2} & \widetilde{v}_{2,2} \\ v_{2,3} & v_{3,3} & \widetilde{v}_{2,3} \end{pmatrix}$$

we have

$$\Delta \equiv 0 \pmod p.$$

On the other hand, from (2.19) we derive that

$$|\Delta| \ll \lambda_1 \lambda_2 \lambda_3 M^7 < \frac{M^{1+o(1)}}{\rho^{16}} < M^{2.6+o(1)}.$$

Hence, $\Delta = 0$, which together with (2.27) implies that the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly dependent, which is impossible.

By (2.23), we have

$$\prod_{i=1}^{3} \lambda_i \le \rho^{-16} M^{-6+o(1)}$$

and since $\lambda_3 > (10M)^{-1}$, we obtain

$$\lambda_1 \lambda_2 < \rho^{-16} M^{-5+o(1)}.$$

We again note that $\lambda_1 > (10M^2)^{-1}$, as otherwise $\mathbf{v}_1$ must have $v_{2,1} = \widetilde{v}_{2,1} = v_{1,1} = \widetilde{v}_{1,1} = 0$. In turn this implies that $v_{3,1} \equiv 0 \pmod p$ and since we assumed that $M = o(p^{1/3})$, we obtain $v_{3,1} = 0$, which contradicts the condition that $\mathbf{v}_1$ is a nonzero vector.

Since $\lambda_1 > (10M^2)^{-1}$ and $\rho > M^{-1/10}$, we get that $\lambda_2 < (10M)^{-1}$. Thus, we have

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \widetilde{v}_{2,i}, 0, 0), \qquad i = 1, 2.$$

Next,

$$\begin{pmatrix} v_{3,1} & \widetilde{v}_{2,1} \\ v_{3,2} & \widetilde{v}_{2,2} \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} -v_{2,1} \\ -v_{2,2} \end{pmatrix} \pmod p.$$

Now we observe that

$$\Delta = \det \begin{pmatrix} v_{3,1} & \widetilde{v}_{2,1} \\ v_{3,2} & \widetilde{v}_{2,2} \end{pmatrix} \ll \lambda_1 \lambda_2 M^5 < \frac{M^{o(1)}}{\rho^{16}}. \tag{2.28}$$

Furthermore,

$$\Delta_1 = \det \begin{pmatrix} -v_{2,1} & \widetilde{v}_{2,1} \\ -v_{2,2} & \widetilde{v}_{2,2} \end{pmatrix} \ll \lambda_1 \lambda_2 M^4 < \frac{M^{-1+o(1)}}{\rho^{16}}, \tag{2.29}$$

and

$$\Delta_2 = \det \begin{pmatrix} v_{3,1} & -v_{2,1} \\ v_{3,2} & -v_{2,2} \end{pmatrix} \ll \lambda_1 \lambda_2 M^5 < \frac{M^{o(1)}}{\rho^{16}}. \tag{2.30}$$

In particular, $|\Delta|, |\Delta_1|, |\Delta_2| < p$. Therefore, if $\Delta \equiv 0 \pmod p$, then $\Delta_1 \equiv \Delta_2 \equiv 0 \pmod p$ and we see that $\Delta = \Delta_1 = \Delta_2 = 0$. Thus, in this case the rank of the matrix formed with vectors $\mathbf{v}_1, \mathbf{v}_2$ is at most 1, which contradicts the linear independence of the vectors $\mathbf{v}_1, \mathbf{v}_2$.

Hence, $\Delta \not\equiv 0 \pmod p$ and we get that

$$c_3 \equiv \frac{\Delta_1}{\Delta} \pmod p, \qquad c_2 \equiv \frac{\Delta_2}{\Delta} \pmod p.$$

We now substitute this in (2.17) and get that

$$\Delta y^2 - a_0 y \equiv \Delta_1 x^3 + \Delta_2 x^2 + b_0 x \pmod p, \qquad |x|, |y| \le M,$$

for some integers a_0, b_0. We observe that the condition $c_3 \not\equiv 0 \pmod p$ implies that $\Delta_1 \neq 0$.

Let now

$$T = \left\lfloor \left(\frac{p}{M}\right)^{1/3} \rho^{16/3} \right\rfloor.$$

Note that $M^{2/3} < T < T^2 < p/2$. By the pigeonhole principle, there exists a positive integer $1 \le t_0 \le T^2 + 1$ such that

$$|(t_0 a_0)_p| \le \frac{p}{T}, \qquad |(t_0 b_0)_p| \le \frac{p}{T},$$

where $(x)_p$ is the element of the residue class $x \pmod p$ with the least absolute value, see also [28, Lemma 3.2]. Hence

$$t_0 \Delta y^2 - (t_0 a_0)_p y \equiv t_0 \Delta_1 x^3 + t_0 \Delta_2 x^2 + (t_0 b_0)_p x \pmod p, \quad |x|, |y| \le M.$$

By (2.28), (2.29), (2.30), the absolute values of the expressions on both sides are bounded by $pM^{1+o(1)}T^{-1}$. Thus, we get

$$t_0 \Delta y^2 - (t_0 a_0)_p y = t_0 \Delta_1 x^3 + t_0 \Delta_2 x^2 + (t_0 b_0)_p x + pz,$$

where

$$|x|, |y| \le M, \quad |z| < M^{1+o(1)} T^{-1}.$$

Now we use Lemma 17 and conclude that the number of solutions is at most

$$\begin{aligned}\left(\frac{M}{T} + 1\right) M^{1/3+o(1)} &< \left(\frac{M^{4/3}}{p^{1/3}} \rho^{-16/3} + 1\right) M^{1/3+o(1)} \\ &< M^{2/3+o(1)} < \left(\frac{M^3}{p}\right)^{1/16} M.\end{aligned}$$

Since the choice for $\varepsilon > 0$ in (2.18) is arbitrary, the result now follows. □

2.2.2 Polynomials of higher degree

Our next result shows that when $\deg f \ge 4$ we also have a non-trivial bound for $|C_f \cap B|$ in the range $M < p^{1/3-\varepsilon}$. To formulate our result, we define $J_{k,m}(H)$ as the number of solutions of the system of m Diophantine equations in $2k$ integral variables $x_1, \dots, x_{2k}$:

$$\begin{cases} x_1^m + \dots + x_k^m &= x_{k+1}^m + \dots + x_{2k}^m, \\ &\vdots \\ x_1 + \dots + x_k &= x_{k+1} + \dots + x_{2k}, \\ 1 \le x_1, \ \dots, \ x_{2k} \le H. \end{cases} \tag{2.31}$$

We also define $\kappa(m)$ to be the smallest integer κ such that for any integer $k \ge \kappa$ there exists a constant $C(k, m)$ depending only on k and m and such that

$$J_{k,m}(H) \le C(k, m) H^{2k - m(m+1)/2 + o(1)}, \tag{2.32}$$

as $H \to \infty$. Note that by a recent result of Wooley [102, Theorem 1.1], that improves the previous estimate of [101], we have $\kappa(m) \le m^2 - 1$ for any $m \ge 3$.

Theorem 10. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree 3 and any square B we have*

$$|C_f \cap B| \le |B|^{1/2+o(1)} \left(\frac{|B|^{3/2}}{p}\right)^{1/2\kappa(m)} + |B|^{1/2 - (m-3)/4\kappa(m) + o(1)}$$

as $|B| \to \infty$.

In particular, for any $\varepsilon > 0$, there exists $\delta > 0$ that depends only on ε and $\deg f$ such that if $M < p^{1/3-\varepsilon}$ and $\deg f \ge 4$, then $|C_f \cap B| \ll |M|^{1/2-\delta}$.

Proof. As before, denote the square $B = [R+1, R+M] \times [S+1, S+M]$. Let $\mathcal{X}$ be the set of integers $x \in [R+1, R+M]$ such that the point (x, y) lies in C_f for some $y \in [S+1, S+M]$. In particular, letting $X = \#\mathcal{X}$ we have

$$|C_f \cap B| \le 2X. \tag{2.33}$$

Fix some integer $k \ge 1$ and consider the set

$$\mathcal{Y}_k = \{y_1^2 + \ldots + y_k^2 \pmod p \ : \ S+1 \le y_i \le S+M, \ i = 1, \ldots, k\}.$$

By making the change of variables $y_i = S + z_i$, $i = 1, \ldots, k$, we observe that

$$\mathcal{Y}_k = \{z_1^2 + \ldots + z_k^2 + 2S(z_1 + \ldots + z_k) + kS^2 \pmod p : \\ 1 \le z_i \le M, \ i = 1, \ldots, k\}.$$

In particular,

$$\#\mathcal{Y}_k \le \#\left\{r + 2Ss + kS^2 \ : \ 1 \le r \le kM^2, \ 1 \le s \le kM\right\} \le k^2M^3.$$

For any $(x_1, \ldots, x_k) \in \mathcal{X}^k$ there exists $\lambda \in \mathcal{Y}_k$ such that

$$f(x_1) + \ldots + f(x_k) \equiv \lambda \pmod p.$$

Thus,

$$X^k \le \sum_{\lambda \in \mathcal{Y}_k} r(\lambda)$$

where

$$r(\lambda) = \#\left\{(x_1, \ldots, x_k) \in [R+1, R+M]^k : f(x_1) + \ldots + f(x_k) \equiv \lambda \pmod p\right\}.$$

Using the Cauchy inequality, we derive

$$X^{2k} \le \#\mathcal{Y}_k \sum_{\lambda \in \mathcal{Y}_k} r^2(\lambda) \le k^2M^3T_k(R, M),$$

where $T_k(R; M)$ is the number of solutions of

$$\begin{cases} f(x_1) + \ldots + f(x_k) \equiv f(x_{k+1}) + \ldots + f(x_{2k}) \pmod p, \\ (x_1, \ldots, x_{2k}) \in [R+1, R+M]^{2k}. \end{cases}$$

The quantity $T_k(R; M)$ has been defined and estimated in [23] for $R = 0$ but making a change of variables, it is clear that the same bound holds for any R. In particular, it is proved in [23] that

$$T_k(R; M) \ll (M^m/p + 1)\, M^{m(m-1)/2} J_{k,m}(M),$$

where, as before, $J_{k,m}(M)$ is the number of solutions of the system of equations (2.31) with $H = M$.

Taking $k = \kappa(m)$ so that the bound (2.32) holds, we derive

$$\begin{aligned} X^{2k} &\le M^3 \left(M^m/p + 1\right) M^{m(m-1)/2} M^{2k - m(m+1)/2 + o(1)} \\ &\le \left(M^m/p + 1\right) M^{2k+3-m+o(1)} \end{aligned}$$

and obtain

$$X \le M(M^3/p)^{1/2\kappa + o(1)} + M^{1-(m-3)/2\kappa + o(1)},$$

which together with (2.33) concludes the proof.

□

2.3 Polynomial values in small boxes

In this section we study those sets of the form:

$$A_f = \{(x, f(x)) : \ x = 1, \dots, p\} \subseteq \mathbb{F}_p \times \mathbb{F}_p$$

and obtain bounds for $|A_f \cap B|$ uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of fixed degree m.

Theorem 11. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree $m \ge 2$ and any square B we have*

$$|A_f \cap B| \ll \frac{|B|}{p} + |B|^{1/2 - 1/2^m} p^{o(1)}$$

as $|B| \to \infty$.

Cilleruelo et al. [23] obtained better estimates (by means of different arguments) for larger degree m, but for $m = 2, 3$ these bounds are better.

Proof. For brevity, in this proof we will denote $J = |A_f \cap B|$ and denote the square $B = [R+1, R+M] \times [S+1, S+M]$. Without loss of generality we can assume that

$$0 \le M + 1 < M + S < p.$$

Applying Lemma 19 to the sequence of fractional parts $\gamma_n = \{f(n)/p\}$, $n = 1, \dots, M$, with

$$\alpha = (S+1)/p, \qquad \beta = (S+M+1)/p, \qquad K = \lfloor p/M \rfloor,$$

so that we have

$$\frac{1}{K} + \min\{\beta - \alpha, 1/k\} \ll \frac{M}{p}$$

for $k = 1, \dots, K$, we derive

$$J \ll \frac{M^2}{p} + \frac{M}{p} \sum_{k=1}^{K} \left| \sum_{n=1}^{M} \exp(2\pi i k f(n)/p) \right|.$$

Therefore, by Lemma 20, we have

$$\begin{aligned} J \ll \frac{M^2}{p} + \frac{M^{2 - m/2^{m-1}}}{p} \\ \times \sum_{k=1}^{K} \left(\sum_{-M < \ell_1, \dots, \ell_{m-1} < M} \min\left\{ M, \left\| \frac{a}{p} m! k \ell_1 \dots \ell_{m-1} \right\|^{-1} \right\} \right)^{2^{1-m}}, \end{aligned}$$

where a is the leading coefficient of f. Now, separating the contribution from the terms with $\ell_1 \dots \ell_{m-1} = 0$ we obtain

$$J \ll \frac{M^2}{p} + \frac{M^{2-m/2^{m-1}}}{p} K (M^{m-1})^{2^{1-m}} + \frac{M^{2-m/2^{m-1}}}{p} W,$$

where

$$W = \sum_{k=1}^{K} \left(\sum_{0<|\ell_1|,\dots,|\ell_{m-1}|<M} \min \left\{ M, \left\| \frac{a}{p} m! k \ell_1 \dots \ell_{m-1} \right\|^{-1} \right\} \right)^{2^{1-m}}.$$

Hence, recalling the choice of K, we derive

$$J \ll \frac{M^2}{p} + M^{1-1/2^{m-1}} + \frac{M^{2-m/2^{m-1}}}{p} W. \tag{2.34}$$

We now will estimate W. Hölder's inequality implies the bound

$$W^{2^{m-1}} \ll K^{2^{m-1}-1} \sum_{k=1}^{K} \sum_{0<|\ell_1|,\dots,|\ell_{m-1}|<M} \min \left\{ M, \left\| \frac{a}{p} m! k \ell_1 \dots \ell_{m-1} \right\|^{-1} \right\}.$$

Collecting together the terms with the same value of

$$z = m! k \ell_1 \dots \ell_{m-1} \not\equiv 0 \pmod p$$

and recalling the well-known bound on the divisor function, we conclude that

$$W^{2^{m-1}} \ll K^{2^{m-1}-1} p^{o(1)} \sum_{\substack{|z|<m!KM^{m-1} \\ z \not\equiv 0 \pmod p}} \min \left\{ M, \left\| \frac{a}{p} z \right\|^{-1} \right\}.$$

Since the sequence $\|am/p\|$ is periodic with period p, we see that

$$\begin{aligned} W^{2^{m-1}} &\ll K^{2^{m-1}-1} p^{o(1)} \frac{KM^{m-1}}{p} \sum_{z=1}^{p-1} \left\| \frac{a}{p} z \right\|^{-1} \\ &= K^{2^{m-1}-1} p^{o(1)} \frac{KM^{m-1}}{p} \sum_{z=1}^{p-1} \left\| \frac{z}{p} \right\|^{-1} \ll K^{2^{m-1}} M^{m-1} p^{o(1)}. \end{aligned}$$

Thus, recalling the choice of K, we derive

$$W \le KM^{(m-1)/2^{m-1}} p^{o(1)} \le M^{(m-1)/2^{m-1}-1} p^{1+o(1)},$$

which after the substitution in (2.34) concludes the proof. □

2.4 Applications

2.4.1 Isomorphism classes of hyperelliptic curves in some thin families

A special case of the equation

$$y^2 \equiv f(x) \pmod p$$

are hyperelliptic curves over $\mathbb{F}_p$. The problem of concentration of points on hyperelliptic curves and polynomial maps is connected with some problems on isomorphisms of hyperelliptic curves that preserve the Weierstrass form. Let g be a fixed positive integer and p be large enough prime (so that $\gcd(p, 2(2g+1)) = 1$), then any hyperelliptic curve can be given by a non-singular Weierstrass equation:

$$H_{\mathbf{a}}: \quad Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1X + a_0,$$

where $\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathbb{F}_p^{2g}$. (we recall that the non-singularity condition is equivalent to non-vanishing of the discriminant of the polynomial $X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1X + a_0$). We refer to [34] for a background on hyperelliptic curves and their applications. From now on, we will identify an hyperelliptic curve $H_{\mathbf{a}}$ with its coefficients vector $\mathbf{a}$.

As we discussed in Section 1.2.3 that isomorphisms of hyperelliptic curves that preserve their Weierstrass form are given by $(x, y) \to (\alpha^2 x, \alpha^{2g+1} y)$ for some $\alpha \in \mathbb{F}_p^*$. Thus $H_{\mathbf{a}}$ is isomorphic to $H_{\mathbf{b}}$, which we denote as $H_{\mathbf{a}} \sim H_{\mathbf{b}}$, if there exists $\alpha \in \mathbb{F}_p^*$ such that

$$a_i \equiv \alpha^{4g+2-2i} b_i \pmod p, \qquad i = 0, \ldots, 2g-1. \tag{2.35}$$

We will study here the isomorphism classes of hyperelliptic curves of genus g over $\mathbb{F}_p$, $H_{\mathbf{a}}$, when $\mathbf{a} = (a_0, \ldots, a_{2g-1})$ belongs to a small $2g$-dimensional cube

$$B = [R_0 + 1, R_0 + M] \times \ldots \times [R_{2g-1} + 1, R_{2g-1} + M] \tag{2.36}$$

with some integers R_j, M satisfying $0 \le R_j < R_j + M < p$, $j = 0, \ldots, 2g-1$. In particular, we note that all components of a vector $\mathbf{a} \in B$ are non-zero modulo p. Our methods below work without this restriction as well, however they somewhat lose their efficiency.

In this section we give an upper bound for the number

$$N(H; B) = \#\{\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in B: \ H_{\mathbf{a}} \sim H\}$$

of hyperelliptic curves $H_{\mathbf{a}}$ with $\mathbf{a} \in B$ that are isomorphic to a given curve H.

First we observe that for large cubes one derives from the Weil bound and Theorem 1 an asymptotic formula

$$N(H; B) = \frac{|B|}{p^{2g-1}} + O\left(p^{1/2}\left(1 + \log_+^{2g}\left(|B|p^{1/2-2g}\right)\right)\right).$$

So we have an asymptotic formula for $N(H; B)$ as long as $|B|/p^{1/2-1/2g} \to \infty$ as $p \to \infty$. However, here we are mostly interested in small cubes.

As before, observe that we always have the trivial upper bound

$$N(H; B) \le 2|B|^{1/2}.$$

To see this, let $H = H_{\mathbf{b}}$, $\mathbf{b} = (b_0, \dots, b_{2g-1}) \in \mathbb{F}_p^{2g}$, be given by a Weierstrass equation. We observe that if $H_{\mathbf{a}} \sim H$ then a_{2g-1} can take at most M values in $\mathbb{F}_p^*$, and each a_{2g-1} determines two possible values for α^2 in (2.35).

It is also useful to remark that one can not expect to get a general bound stronger than

$$N(H; B) = O(M^{1/(2g+1)}).$$

To see this we consider the set $\mathcal{Q}$ of quadratic residues modulo p in the interval $[1, M^{1/(2g+1)}]$. It is well-known that for almost all primes p (that is, for all except a set of relative density zero) we have

$$\#\mathcal{Q} \sim 0.5M^{1/(2g+1)}, \qquad \text{as } M \to \infty.$$

For example, this follows from a bound of Heath-Brown [55, Theorem 1] on average values of sums of real characters.

Consider now the set

$$\mathcal{A} = \{\alpha \in \mathbb{F}_p \ : \ \alpha^2 \in \mathcal{Q}\},$$

the curve $H : Y^2 = X^{2g+1} + X^{2g-1} + X^{2g-2} + \ldots + X + 1$ and the $2g$-dimensional cube $B = [1, M]^{2g}$. It is clear that $(\alpha^4, \alpha^6, \dots, \alpha^{4g+2}) \in B$ for all $\alpha \in \mathcal{A}$. On the other hand $\#\mathcal{A} = 2\#\mathcal{Q} \sim M^{1/(2g+1)}$.

First observe that, in the case of elliptic curves (that is $g + 1$), the quantity $N(E; B)$ for some elliptic curve

$$E : \ Y^2 = X^3 + aX + b$$

over $\mathbb{F}_p$ with coefficients $a, b \in \mathbb{F}_p^*$, can be bounded by the number of pairs $(r, s) \in B$ satisfying

$$r^3 \equiv \lambda s^2 \pmod p,$$

where $\lambda \equiv a^3 b^{-2} \in \mathbb{F}_p^*$. In particular, bounds from Corollary 7 apply to $N(E; B)$ as long as the box $B = [R + 1, R + M] \times [S + 1, S + M]$ satisfies the condition

$$R, S > 0, \ R + M, S + M < p.$$

A simple observation shows that in the case of hyperelliptic curves with $g \geq 2$ the quantity $N(H; B)$ is closely related to the problem of concentration of points of a quadratic polynomial map. Then one can apply the general result of [23] and get a non-trivial upper bound for $N(H; B)$ for any range of M. However, here we use a different approach and we obtain a better bound.

Using (2.35), Theorem 11 and the bound from [23, Theorem 3]

$$|A_f \cap B| \ll |B|^{1/2m+o(1)} \tag{2.37}$$

that holds for $M \leq p^{2/(m^2+3)}$, we derive the following consequence.

Theorem 12. *For any hyperelliptic curve H of genus $g \geq 2$ over $\mathbb{F}_p$ and cube B non-intersecting the axes (see (2.36)), we have*

$$N(H; B) \ll \frac{|B|}{p} + |B|^{1/4+o(1)}.$$

Proof. Assume that $H = H_{\mathbf{b}}$ for some vector $\mathbf{b} = (b_0, \dots, b_{2g-1}) \in \mathbb{F}_p^{2g}$. We recall that all components of any vector $\mathbf{a} \in B$ are non-zero modulo p. Hence, $b_0 \in \mathbb{F}_p^*$ and we see from (2.35) (combining the equations with $i = 2g+1-h$ and $i = 2g-1$) that

$$\begin{aligned} a_{2g-1}^h \equiv & \lambda a_{2g+1-h}^2 \pmod p, \\ R_{2g+1-h} + 1 \le & a_{2g+1-h} \le R_{2g+1-h} + M, \\ R_{2g-1} + 1 \le & a_{2g-1} \le R_{2g-1} + M, \end{aligned} \tag{2.38}$$

where

$$\lambda = b_{2g-1}^h / b_{2g+1-h}^2. \tag{2.39}$$

We also observe that

$$\alpha^4 = b_{2g-1}/a_{2g-1}.$$

Thus, each solution (a_{g+1-h}, a_{2g-1}) of (2.38) determines at most two values of α^2, each of which in turn determines all other values of $a_0, a_1, \dots, a_{2g-1}$.

Thus we have seen that $N(H;B) \le 2T$, where T is the number of solutions (x,y) of the congruence

$$x^h \equiv \lambda y^2 \pmod p, \quad R+1 \le x \le R+M,\ S+1 \le y \le S+M, \tag{2.40}$$

where $R = R_{g+1-h}$, $S = R_{2g-1}$ and λ is given by (2.39).

We now observe that the congruence (2.40) taken with $h = 4$, which is admissible for $g \ge 2$, implies

$$x^2 \equiv \mu y \pmod p, \quad R+1 \le x \le R+M,\ S+1 \le y \le S+M,$$

where μ is one of the two square roots of λ (we recall that $g \ge 2$). Applying Theorem 11 for $M > p^{2/7}$ and also (2.37) for $M \le p^{2/7}$ with a quadratic polynomial f, we immediately obtain the desired result. □

Using the idea of the proof of Theorem 8, we establish the following result which is valid for any hyperelliptic curve (including elliptic curves).

Theorem 13. *For any hyperelliptic curve H of genus $g \ge 1$ over $\mathbb{F}_p$, any cube B non-intersecting the axes (see (2.36)) and any odd integer $h \in [3, 2g+1]$, we have*

$$N(H;B) < \left(|B|^{1/2h} + |B|^{1/2}\left(|B|^2/p\right)^{2/h(h+1)}\right)|B|^{o(1)},$$

as $|B| \to \infty$.

We observe that if $M < p^{1/(2g^2+2g+4)}$ then, taking $h = 2g+1$ in Theorem 13, we obtain the estimate $N(H;B) \le M^{1/(2g+1)+o(1)}$ which, as we have seen, is sharp up to the $o(1)$ term.

Proof. As in the proof of Theorem 12 we let $H = H_{\mathbf{b}}$ for some $\mathbf{b} = (b_0, \dots, b_{2g-1}) \in \mathbb{F}_p^{2g}$.

We can assume that $M < p^{1/4}$ as otherwise the results are weaker than the trivial upper bound $N(H;B) \ll M$.

Let T be the number of solutions (x,y) to the congruence (2.40).

We follow the proof of Theorem 8. We can assume that T is sufficiently large (recall that g is fixed integer constant). We fix some integer L with

$$1 \le L \le \frac{T}{12(h+1)}, \tag{2.41}$$

to be chosen later. Thus, there exists Q such that the congruence

$$x^h \equiv \lambda y^2 \pmod p, \qquad Q+1 \le x \le Q+M/L,\ S+1 \le y \le S+M,$$

has at least T/L solutions. We can split the interval $[Q+1, Q+M/L]$ into $k_0 = \lfloor T/(6(h+1)L) \rfloor$ intervals of length at most $6(h+1)M/T$. Since there are at most two solutions to the above congruence with the same value of x, and since we have at least $T/L > 4(h+1)k_0$ solutions in total, from the pigeonhole principle it follows that there exists an interval of length $6(h+1)M/T$ containing at least $2(h+1)$ pairwise distinct values of x. Let x_0 be the first of these values and (x_0, y_0) the solution. It is clear that T/L is bounded by the number of solutions of

$$\begin{cases} (x_0+x)^h \equiv \lambda (y_0+y)^2 \pmod p, \\ -M/L \le x \le M/L, \quad -M \le y \le M, \end{cases}$$

which is equivalent to

$$\begin{cases} c_h x^h + \ldots + c_1 x + c_0 y \equiv y^2 \pmod p, \\ -M/L \le x \le M/L, \quad -M \le y \le M, \end{cases} \tag{2.42}$$

where

$$c_0 = -2y_0 \text{ and } c_j = \lambda^* \binom{h}{j} x_0^{h-j},\ j = 1, \ldots, h,$$

where λ^* is defined by $\lambda^* \lambda \equiv 1 \pmod p$ and $1 \le \lambda^* < p$. In particular, $c_h \not\equiv 0 \pmod p$. Besides, there are at least $2h+1$ solutions (x, y) of (2.42) with x pairwise distinct and such that $1 \le x \le 6(h+1)M/T$. From these $2h+1$ values we fix h: $(x_1, y_1), \ldots, (x_h, y_h)$ and rewrite (2.42) in the form

$$\begin{pmatrix} x^h & \ldots & x & y \\ x_h^h & \ldots & x_h & y_h \\ & \ldots & & \\ x_1^h & \ldots & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_h \\ \ldots \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y^2 \\ y_h^2 \\ \ldots \\ y_1^2 \end{pmatrix} \pmod p. \tag{2.43}$$

Since h is odd, by Lemma 25, we know that at most $2h$ pairs (x, y), with x pairwise distinct, satisfy both the congruence (2.43) and the congruence

$$\begin{vmatrix} x^h & \ldots & x & y \\ x_h^h & \ldots & x_h & y_h \\ & \ldots & & \\ x_1^h & \ldots & x_1 & y_1 \end{vmatrix} \equiv 0 \pmod p.$$

Since there are at least $2h+1$ solutions of (2.43), for one of them, say (x_{h+1}, y_{h+1}), we have

$$\Delta = \begin{vmatrix} x_{h+1}^h & \ldots & x_{h+1} & y_{h+1} \\ x_h^h & \ldots & x_h & y_h \\ & \ldots & & \\ x_1^h & \ldots & x_1 & y_1 \end{vmatrix} \not\equiv 0 \pmod p.$$

Note that $1 \le |\Delta| \ll (M/T)^{h(h+1)/2}M$. Now we solve the system

$$\begin{pmatrix} x_{h+1}^h & \dots & x_{h+1} & y_{h+1} \\ x_h^h & \dots & x_h & y_h \\ & \dots & & \\ x_1^h & \dots & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_h \\ c_{h-1} \\ \dots \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_{h+1}^2 \\ y_h^2 \\ \dots \\ y_1^2 \end{pmatrix} \pmod p$$

with respect to $(c_h, \dots, c_1, c_0)$. We write Δ_j for the determinant of the matrix on the left hand side where we have substituted the column j by the vector $(y_{h+1}^2, \dots, y_1^2)$. With this notation we have that

$$c_j = \frac{\Delta_{h+1-j}}{\Delta}, \quad j = 0, \dots h,$$

and the congruence (2.42) is equivalent to

$$\Delta_1 x^h + \Delta_2 x^{h-1} + \ldots + \Delta_h x + \Delta_{h+1} y - \Delta y^2 \equiv 0 \pmod p.$$

In particular, $\Delta_1 \not\equiv 0 \pmod p$. We can write this congruence as an equation over $\mathbb{Z}$:

$$\Delta_1 x^h + \Delta_2 x^{h-1} + \ldots + \Delta_h x + \Delta_{h+1} y - \Delta y^2 = pz, \qquad z \in \mathbb{Z}. \tag{2.44}$$

We can easily check that

$$|\Delta_{h+1}| \ll (M/T)^{h(h+1)/2} M^2$$

and

$$|\Delta_j| \ll (M/T)^{h(h-1)/2+j-1} M^3, \qquad j = 1, \dots, h.$$

Thus, collecting the above estimates, we derive

$$\begin{aligned} |z| &\ll \frac{1}{p} \left(\sum_{j=1}^{h} |\Delta_j| (M/L)^{h-j+1} + |\Delta_{h+1}| M + |\Delta| M^2 \right) \\ &\ll \frac{M^3}{p} \left(\sum_{j=1}^{h} (M/T)^{h(h-1)/2+j-1} (M/L)^{h-j+1} + (M/T)^{h(h+1)/2} \right) \\ &\ll \frac{M^3}{p} \left(M^{h(h+1)/2} T^{-h(h-1)/2} L^{-h} \sum_{j=1}^{h} (T/L)^{-j+1} + (M/T)^{h(h+1)/2} \right) \\ &\ll \frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2} L^h}. \end{aligned}$$

since by (2.41) we have

$$\sum_{j=1}^{h} (T/L)^{-j+1} = O(1) \text{ and } (M/T)^{h(h+1)/2} \le \frac{M^{h(h+1)/2}}{T^{h(h-1)/2} L^h}.$$

Since h is odd, and $\Delta \ne 0$, $\Delta_1 \ne 0$, we have that, for each z, the curve (2.44) is absolutely irreducible. Thus by Lemma 17 it contains at most $M^{1/h+o(1)}$ integer points (x, y) with $|x|, |y| \le M$. Hence

$$T \le L M^{1/h+o(1)} \left(1 + \frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2} L^h} \right) \tag{2.45}$$

for any L satisfying (2.41).

We can assume that the following lower bounds hold for T:

$$T > M^{1/h} \text{ and } T > 24(h+1)\left(M(M^4/p)^{2/h(h+1)} + 1\right) \tag{2.46}$$

since otherwise there is nothing to prove.

Take $L = \left\lfloor 1 + (M^{(h^2+7)/2}/p)^{2/h(h+1)} \right\rfloor$. We note that (2.41) holds as otherwise $L \geq 2$ and we have

$$\left(\frac{M^{(h^2+7)/2}}{p}\right)^{2/h(h+1)} \geq L - 1 \geq \frac{L}{2} > \frac{T}{24(h+1)} > M\left(\frac{M^4}{p}\right)^{2/h(h+1)},$$

which is impossible.

If $M < p^{2/(h^2+7)}$ we have $L = 1$ and in view of (2.46), also

$$\frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h} \leq \frac{M^{h(h+1)/2+3}}{pM^{(h-1)/2}} = \frac{M^{(h^2+7)/2}}{p} < 1$$

In this case, the bound (2.45) yields

$$T \ll M^{1/h+o(1)}.$$

If $M \geq p^{2/(h^2+7)}$, we have

$$(M^{(h^2+7)/2}/p)^{2/h(h+1)} \ll L \ll (M^{(h^2+7)/2}/p)^{2/h(h+1)}$$

and, recalling our assumption (2.46) we obtain

$$\frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h} \ll \frac{M^{h(h+1)/2+3}}{pM^{h(h-1)/2}(M^4/p)^{(h-1)/(h+1)}(M^{(h^2+7)/2}/p)^{2/(h+1)}} = 1.$$

Hence, in this case we derive from (2.45) that

$$T \leq (M^{(h^2+7)/2}/p)^{2/h(h+1)} M^{1/h+o(1)} = M\left(M^4/p\right)^{2/h(h+1)+o(1)},$$

which concludes the proof.

□

2.4.2 Number of isomorphism classes

In [81], the author obtained a formula for the number of hyperelliptic curves of genus g over a finite field $\mathbb{F}_q$ of odd characteristic, expressed as a polynomial in q. In particularthat, his result implies that the number of non isomorphic hyperelliptic curves of genus g over $\mathbb{F}_p$ is $2p^{2g-1} + O(gp^{2g-2})$.

We address here the problem of estimating from below the number of non-isomorphic hyperelliptic curves of genus g over $\mathbb{F}_p$, $H_{\mathbf{a}}$, when $\mathbf{a} = (a_0, \ldots, a_{2g-1})$ belongs to a small $2g$-dimensional cube B non-intersecting the axes. In particular, we note that all components of a vector $\mathbf{a} \in B$ are non-zero modulo p.

Let $\mathcal{H}(B)$ be the collection of representatives of all isomorphism classes of hyperelliptic curves $H_{\mathbf{a}}$, $\mathbf{a} \in B$, where B is a $2g$-dimensional cube of side length M. Certainly the upper bounds of our theorems lead to a lower bound on $\#\mathcal{H}(B)$. However, using a different approach we obtain a near optimal bound for the number of isomorphism classes.

Theorem 14. *For $g \ge 1$ and any cube B non-intersecting the axes (see (2.36)), we have*

$$\#\mathcal{H}(B) \gg_g \min\left\{p^{2g-1}, |B|^{1+o(1)}\right\},$$

as $|B| \to \infty$. Furthermore, if $g \ge 2$ the $o(1)$ term can be removed when $|B| > p$.

Proof. Clearly

$$\sum_{H \in \mathcal{H}(B)} N(H;B) = M^{2g}. \tag{2.47}$$

We also set

$$T(B) = \sum_{H \in \mathcal{H}(B)} N(H;B)^2. \tag{2.48}$$

Using (2.47), (2.48) and the Cauchy inequality we derive

$$\#\mathcal{H}(B) \ge M^{4g} T(B)^{-1}.$$

We observe that $T(B)$ is the number of pairs of vectors $(\mathbf{a}, \mathbf{b})$, $\mathbf{a}, \mathbf{b} \in B$, such that there exists α such that

$$a_i \equiv \alpha^{4g+2-2i} b_i \pmod p, \qquad i = 0, \dots, 2g-1.$$

In particular,

$$a_{2g-1}^3 b_{2g-2}^2 \equiv a_{2g-2}^2 b_{2g-1}^3 \pmod p.$$

Now by Theorem 30, we see that there are only $O\left(M^4/p + M^{2+o(1)}\right)$ possibilities for the quadruple $(a_{2g-1}, a_{2g-2}, b_{2g-1}, b_{2g-2})$. When it is fixed, the parameter α in (2.35) can take at most 4 values, and thus for every choice of $(a_0, \dots, a_{2g-3})$ there are only 4 choices for $(b_0, \dots, b_{2g-3})$. Therefore,

$$T(B) \le M^{2g-2}\left(M^4/p + M^{2+o(1)}\right).$$

When $M < p^{1/(2g)}$ we obtain $T(B) \le M^{2g+o(1)}$ and $\#\mathcal{H}(B) \ge M^{2g+o(1)}$, which proves Theorem 14 in this range.

When $M \ge p^{1/(2g)}$ we use a different approach. Using the notation

$$N_i(\lambda) = \#\{(a_i, b_i) \ : \ a_i/b_i \equiv \lambda \pmod p,\ R_i + 1 \le a_i, b_i \le R_i + M\},$$

we can write

$$T(B) = \sum_{\alpha=1}^{p-1} N_0(\alpha^{4g+2}) N_1(\alpha^{4g}) \dots N_{2g-1}(\alpha^4).$$

Thus,

$$\begin{aligned} T(B)^{2g} &\le \left(\sum_{\alpha=1}^{p-1} N_0^{2g}(\alpha^{4g+2})\right) \dots \left(\sum_{\alpha \ne 0} N_{2g-1}^{2g}(\alpha^4)\right) \\ &\le \left((4g+2)\sum_{\alpha=1}^{p-1} N_0^{2g}(\alpha)\right) \dots \left(4\sum_{\alpha=1}^{p-1} N_{2g-1}^{2g}(\alpha)\right) \end{aligned}$$

and then we have

$$T(B) \ll \max_i \sum_{\alpha=1}^{p-1} N_i^{2g}(\alpha).$$

We observe that for any $\alpha \not\equiv 0 \pmod p$ there exist integers r, s with $1 \le |r|, s \le p^{1/2}$, $(r,s)=1$ and such that $\alpha \equiv r/s \pmod p$. Thus

$$\sum_{\alpha=1}^{p-1} N_i^{2g}(\alpha) \le \sum_{\substack{1\le r,s<p^{1/2}\\ \gcd(r,s)=1}} N_i^{2g}(r/s) + \sum_{\substack{1\le r,s<p^{1/2}\\ \gcd(r,s)=1}} N_i^{2g}(-r/s).$$

We observe that $N_i(r/s)$ is the number of solutions (x,y) to the congruence

$$x/y \equiv r/s \pmod p, \qquad R_i + 1 \le x, y \le R_i + M,$$

which, after the change of variables, is equivalent to the congruence

$$sx - ry \equiv c \pmod p, \quad 1 \le x, y \le M,$$

for a suitable c. We can write the congruence as an equation in integers

$$sx - ry = c + zp, \quad 1 \le x, y \le M, \quad z \in \mathbb{Z}.$$

We observe that

$$|z| \le \frac{|s|M + |r|M + |c|}{p} \le \frac{(|s| + |r|)M}{p} + 1.$$

For each z we consider, in case it has, a solution (x_z, y_z), $1 \le x_z, y_z \le M$. The solutions of the Diophantine equation above is given by $(x,y) = (x_z + rt, y_z + st)$, $t \in \mathbb{Z}$. The restriction $1 \le x, y \le M$ implies that $|t| \le M/\max\{r,s\}$.

Thus we have

$$\begin{aligned} N_i(r/s) &\le \left(1 + \frac{2M}{\max\{r,s\}}\right)\left(1 + \frac{2M(s+r)}{p}\right) \\ &\le 1 + \frac{4M\max\{r,s\}}{p} + \frac{2M}{\max\{r,s\}} + \frac{4M^2}{p}. \end{aligned}$$

Therefore

$$\begin{aligned} &\sum_{\substack{1\le r,s<p^{1/2}\\ \gcd(r,s)=1}} N_i^{2g}(r/s) \\ &\quad\ll \sum_{1\le r,s<p^{1/2}} \left(1 + \frac{M^{2g}(\max\{r,s\})^{2g}}{p^{2g}} + \frac{M^{2g}}{(\max\{r,s\})^{2g}} + \frac{M^{4g}}{p^{2g}}\right) \\ &\quad\ll \sum_{1\le r<s<p^{1/2}} \left(1 + \frac{M^{2g}s^{2g}}{p^{2g}} + \frac{M^{2g}}{s^{2g}} + \frac{M^{4g}}{p^{2g}}\right) \\ &\quad\ll \sum_{1\le s<p^{1/2}} \left(s + \frac{M^{2g}s^{2g+1}}{p^{2g}} + \frac{M^{2g}}{s^{2g-1}} + \frac{M^{4g}s}{p^{2g}}\right) \\ &\quad\ll p + \frac{M^{2g}}{p^{g-1}} + M^{2g}\sum_{1\le s<p^{1/2}} \frac{1}{s^{2g-1}} + \frac{M^{4g}}{p^{2g-1}}. \end{aligned}$$

The estimate of the sum with $N_i^{2g}(-r/s)$ is fully analogous.

Assume that $M \geq p^{1/(2g)}$ and observe that

$$\sum_{1 \leq s < p^{1/2}} \frac{1}{s^{2g-1}} \ll \begin{cases} \log M, & \text{if } g = 1, \\ 1, & \text{if } g \geq 2. \end{cases}$$

Thus we have

$$T(B) \ll \begin{cases} M^2 \log M + M^4/p, & \text{if } g = 1, \\ M^{2g} + M^{4g}/p^{2g-1}, & \text{if } g \geq 2, \end{cases} \tag{2.49}$$

which gives

$$\#\mathcal{H}(B) \geq M^{4g} T(B)^{-1} \gg \begin{cases} \min\{p, M^{2+o(1)}\}, & \text{if } g = 1, \\ \min\{p^{2g-1}, M^{2g}\}, & \text{if } g \geq 2, \end{cases}$$

and proves Theorem 14 in the range $M \geq p^{1/2g}$. □

2.4.3 Number of isogeny classes for elliptic curves

Similar ideas can be exploited to obtain lower bounds for the cardinality of the set $\mathcal{I}(\mathcal{B})$ of non-isomorphic isogenous elliptic curves $H_{\mathbf{a}}$ with coefficients in a cube $\mathcal{B}$.

Indeed, let us denote by $\mathcal{I}_t$ the isogeny class consisting of elliptic curves over $\mathbb{F}_p$ with the same number $p+1-t$ of $\mathbb{F}_p$-rational points. By a result of Deuring [36], each admissible value of t, that is, with $|t| \leq 2p^{1/2}$, is taken and hence there are $4p^{1/2}$ isogeny classes. Furthermore, Birch [6] has actually given a formula via the Kronecker class number for the number of isomorphism classes of elliptic curves over a finite field $\mathbb{F}_q$ lying in $\mathcal{I}_t$. Finally, Lenstra [67] has obtained upper and lower bounds for this number and, in particular, shown that

$$\#\mathcal{I}_t \ll p^{1/2} \log p \, (\log \log p)^2 . \tag{2.50}$$

Observe that once again bounds for $N(H; B)$ can be translated into bounds for the number of isogenous non-isomorphic curves with coefficients in B, via multiplication by $p^{1/2+o(1)}$. However, as we have done before, one can obtain better bounds in terms of $T(B)$ which is given by (2.48).

Thus, using (2.49), with $g = 1$, and also (2.50), we see that for the set $\mathcal{H}(t, B)$ of elliptic curves $H_{\mathbf{a}} \in \mathcal{I}_t$ with $\mathbf{a} \in B$, we have

$$\begin{aligned} \#\mathcal{H}(t, B) &= \sum_{H \in \mathcal{H}(B) \cap \mathcal{I}_t} N(H, B) \\ &\leq (\#\mathcal{I}_t)^{1/2} \left(\sum_{H \in \mathcal{H}(B)} N(H, B)^2 \right)^{1/2} = (\#\mathcal{I}_t)^{1/2} T(B)^{1/2} \\ &\ll \left(M^2 p^{-1/4} + p^{1/4} M \log^{1/2} M \right) (\log p)^{1/2} \log \log p. \end{aligned}$$

This improves the trivial bound

$$\#\mathcal{H}(t, B) \ll \min\{M^2, p^{3/2} \log p (\log \log p)^2\}$$

(it follows from (2.50) that there are at most $O(p^{3/2}\log p(\log\log p)^2)$ Weierstrass equations of elliptic curves in the same isogeny class), for $p^{1/4+\varepsilon} \le M \le p^{7/8-\varepsilon}$ with any fixed $\varepsilon > 0$. Furthermore, it also implies the lower bound

$$\begin{aligned}\#\mathcal{I}(\mathcal{B}) &\gg \frac{M^2}{\max_{|t|\in 2p^{1/2}} \mathcal{H}(t,B)}\\ &\gg \min\{p^{1/4}, Mp^{-1/4}\log^{-1/2} M\}(\log p)^{-1/2}(\log\log p)^{-1}.\end{aligned}$$

2.4.4 Diameter of polynomial dynamical systems

Results about concentration of points on curves are also closely related to the question about the diameter of partial trajectories of polynomial dynamical systems. Namely, given a polynomial $f \in \mathbb{F}_p[X]$ and an element $u_0 \in \mathbb{F}_p$, we consider the sequence of elements of $\mathbb{F}_p$ generated by iterations $u_n = f(u_{n-1})$, $n = 0, 1, \ldots$. Clearly the sequence u_n is eventually periodic. In particular, let T_{f,u_0} be the full trajectory length, that is, the smallest integer t such that $u_t = u_s$ for some $s < t$. The study of the diameter

$$D_{f,u_0}(N) = \max_{0\le k,s\le N-1} |u_k - u_s|$$

has been initiated in [54] and then continued in [13, 14, 23]. In particular, it follows from [54, Theorem 6] that for any fixed ε, for $T_{f,u_0} \ge N \ge p^{1/2+\varepsilon}$ we have the asymptotically best possible bound

$$D_{f,u_0}(N) = p^{1+o(1)}$$

as $p \to \infty$. For smaller values of N a series of lower bounds on $D_{f,u_0}(N)$ is given in [13, 14, 23].

One easily derives from Theorem 11 the following estimate, which improves several previous results to intermediate values of N (and is especially effective for small values of m).

Corollary 8. *For any polynomial $f \in \mathbb{F}_p[X]$ of degree $m \ge 2$ and positive integer $N \le T_{f,u_0}$, we have*

$$D_{f,u_0}(N) \gg \min\left\{N^{1/2}p^{1/2}, N^{1+1/(2^{m-1}-1)}p^{o(1)}\right\},$$

as $p \to \infty$.

Proof. Consider the pairs $(u_n, u_{n+1}) = (u_n, f(u_n)) \in A_f$. Since $N \le T_{f,u_0}$, it is clear that all pairs are distinct and, in fact, they belong to the square:

$$B = [u_0 - D_{f,u_0}(N), u_0 + D_{f,u_0}(N)] \times [u_0 - D_{f,u_0}(N), u_0 + D_{f,u_0}(N)].$$

It follows from Theorem 11 that

$$N \le |A_f \cap B| \ll \frac{|B|}{p} + |B|^{1/2-1/2^m}p^{o(1)},$$

which concludes the proof since $|B| = 4D_{f,u_0}(N)^2$. □

On the other hand, we remark that our method and results do not affect the superpolynomial lower bounds of [13, 14] that hold for small values of N.

Part II

Questions regarding sequences of numbers

▲

Various problems in additive combinatorics

Chapter 3

The least common multiple of sets of positive integers

The first important attempt to prove the Prime Number Theorem was made by Chebyshev. In 1853 [18] he introduced the function

$$\psi(n) = \sum_{p^m \leq n} \log p$$

and proved that the Prime Number Theorem was equivalent to the asymptotic estimate $\psi(n) \sim n$. He also proved that if $\psi(n)/n$ had a limit as n tends to infinity then that limit had to be 1. The proof of such convergence result was only completed (independently) two years after Chebyshev's death by Hadamard and de la Vallée Poussin.

Observe that Chebyshev's function is precisely $\psi(n) = \log \operatorname{lcm}(1, 2, \ldots, n)$, so it seems natural to consider the following question: for a given set of integers $S \subseteq [1, n]$, what can be said about the $\log \operatorname{lcm}\{a : a \in S\}$? As Hadamard and de la Vallée Poussin proved, for $S = \{1, \ldots, n\}$, this quantity asymptotically behaves like n.

Some progress has been made in the direction of generalizing this result to a broader class of sets, specially from those sets arising from polynomial sequences. Exploiting the Prime Number Theorem for arithmetic progressions one can get the asymptotic estimate for any linear polynomial $f(x) = ax + b$, see for example [3]. In fact

$$\log \operatorname{lcm}(a + b, 2a + b, \ldots, na + b) \sim n \frac{q}{\varphi(q)} \sum_{\substack{k=1 \\ (k,q)=1}}^{q} \frac{1}{k},$$

where $q = a/\gcd(a, b)$. Recently, Cilleruelo [20] extended this result to the quadratic case and obtained that, for an irreducible polynomial $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$, the following asymptotic estimate holds:

$$\log \operatorname{lcm}(f(1), f(2), \ldots, f(n)) = n \log n + Bn + o(n), \tag{3.1}$$

where the constant $B = B_f$ is an explicit constant that depends on the discriminant of f. The author also proves that for reducible polynomials of degree two, the asymptotic is linear in n. The same ideas can be exploited to obtain the asymptotic for products of linear polynomials which was studied in [60].

An important ingredient in Cilleruelo's argument is a result of Tóth [95], a generalization of a deep theorem of Duke, Friedlander and Iwaniec [38] about the distribution of solutions of quadratic congruences $f(x) \equiv 0 \pmod{p}$, when p runs over all primes. A recent application of the latter result in the negative discriminant case [59] allowed us to sharpen the error term of expression (3.1) in a special case.

In Section 3.1 we focus our study on the particular polynomial $f(x) = x^2 + 1$, which simplifies the calculations and shows how the method developed in [20] works in a clear manner. The same ideas could be extended to general irreducible quadratic polynomials with negative discriminant, however, a generalization of [59] (in the same direction as Tóth's) would be necessary.

For this particular polynomial the expression for B in (3.1) is given by

$$\gamma - 1 - \frac{\log 2}{2} - \sum_{p \neq 2} \frac{\left(\frac{-1}{p}\right) \log p}{p-1} \approx -0.0662756342, \tag{3.2}$$

where γ denotes the Euler constant, $\left(\frac{-1}{p}\right)$ the Legendre symbol and the sum is taken over all odd prime numbers (B can be computed with high numerical precision by using its expression in terms of L-series and zeta-series, see [20] for details). More precisely, we obtain the following estimate.

Theorem 15. *For any $\theta < 4/9$ we have*

$$\log \operatorname{lcm}(1^2+1, 2^2+1, \ldots, n^2+1) = n \log n + Bn + O\left(\frac{n}{(\log n)^\theta}\right),$$

where the constant B is given by Expression (3.2).

Recall that the infinite sum in (3.2) appears in other mathematical contexts: as Moree pointed in [79] this sum is closely related to multiplicative sets whose elements are non-hypotenuse numbers (i.e. integers which could not be written as the hypotenuse of a right triangle with integer sides).

Unfortunately, these ideas cannot be extended to higher degree polynomials and nothing is known for $\log \operatorname{lcm}(f(1), \ldots, f(n))$ when f is an irreducible polynomial of degree greater than 2. For example, nothing is known about the asymptotic of $\log \operatorname{lcm}(1^3+2, 2^3+2, \ldots, n^3+2)$, and then it is natural to wonder what should we expect this quantity to be.

Heuristic arguments and computations allowed Cilleruelo to state the following conjecture.

Conjecture 1 (Cilleruelo [20])**.** *Let $f \in \mathbb{Z}[x]$ be any irreducible polynomial of degree $\deg(f) \geq 3$, then*

$$\log \operatorname{lcm}(f(1), f(2), \ldots, f(n)) \sim (\deg(f) - 1) n \log n.$$

Observe that for two polynomials with similar growth, such as $f_1(x) = x^2 + 1$ or $f_2(x) = x^2 - 1$, the asymptotics obtained are $n \log n$ on the former case and n on the latter. In both cases the given sets have n elements in $[1, n^2 + 1]$, but clearly different arithmetical properties, so: what should one expect -in terms of the lcm- when choosing n elements at random from $[n^2]$?

In Section 3.2 we study this question and show that for almost all sets $S \subseteq [1, n^2]$ of n elements the asymptotic for

$$\psi(S) = \log \operatorname{lcm}\{a : \ a \in S\}$$

is $n \log n$, and therefore coincides in this sense with the irreducible polynomial case.

In fact, we deal with a more general problem. For a given positive integer $k = k(n)$, typically a function of n, we consider the probabilistic model where each subset of k elements is chosen uniformly at random among all sets of size k in $[n] = \{1, \dots, n\}$. We will denote by $\binom{[n]}{k}$ the family of such subsets and denote this model by $S(n, k)$.

Theorem 16. *For $k = k(n) < n$ and $k \to \infty$ we have, for some positive constant C,*

$$\psi(S) = k \frac{\log(n/k)}{1 - k/n} \left(1 + O(e^{-C\sqrt{\log k}})\right)$$

almost surely in $S(n, k)$ when $n \to \infty$.

We also consider another natural probabilistic model, denoted by $B(n, \delta)$, where each element in S is chosen independently at random in $\{1, \dots, n\}$ with probability $\delta = \delta(n)$, again typically a function of n, and proof the following result.

Theorem 17. *If $\delta = \delta(n) < 1$ and $\delta n \to \infty$ then*

$$\psi(S) \sim n \frac{\delta \log(\delta^{-1})}{1 - \delta}$$

asymptotically almost surely in $B(n, \delta)$.

When $\delta = 1/2$ all the subsets $A \subset \{1, \dots, n\}$ are chosen with the same probability, that is 2^{-n}, and Theorem 17 gives the following result.

Corollary 9. *For almost all sets $S \subset \{1, \dots, n\}$ we have that*

$$\operatorname{lcm}\{a : \ a \in A\} = 2^{n(1+o(1))}.$$

When $\delta = k/n$ the heuristic suggests that both models are quite similar. Indeed, this is the strategy we follow in Section 3.2 to prove Theorem 16 via Theorem 17

Observe that the cases $k = n$ in $S(n, k)$ and $\delta = 1$ in $B(n, \delta)$, which are not included in the previous results, correspond to Chebyshev's function and its asymptotic estimate appears as the limiting case, since $\lim_{k/n \to 1} \frac{\log(n/k)}{1 - k/n} = \lim_{\delta \to 1} \frac{\delta \log(\delta^{-1})}{1 - \delta} = 1$.

3.1 The logarithm of the lcm of a quadratic sequence

Let us first recall some preliminary results and notation:

$$\begin{aligned}\pi(n) &= |\{p : p \le n\}|,\\ \pi_1(n) &= |\{p : p \equiv 1 \pmod 4, p \le n\}|,\\ \pi_1([a,b]) &= |\{p : p \equiv 1 \pmod 4, a < p \le b\}|.\end{aligned}$$

The Prime Number Theorem states that the following estimate holds:

$$\psi(n) = \log \operatorname{lcm}(1,2,\dots,n) = n + E(n),\ E(n) = O\left(\frac{n}{(\log n)^{\kappa}}\right), \tag{3.3}$$

where κ can be chosen as large as necessary. We also use the following estimate, which follows from the Prime Number Theorem for arithmetic progressions:

$$\pi_1(n) = \frac{n}{2\log n} + O\left(\frac{n}{(\log n)^2}\right). \tag{3.4}$$

The content of this chapter follows the lines of [20] and some its parts has been included for sake of completeness. We will first identify those primes appearing in the $\operatorname{lcm}(1^2+2,\dots,n^2+1)$ by comparing this quantity with the product $\prod_{k=1}^{n}(k^2+1)$. This will give us the precise contribution for those primes greater than $2n$ and leave us with the study of the *small* primes ($p \le n^{2/3}$) in Lemma 5 and the *medium* primes ($n^{2/3} < p \le 2n$) in Section 3.1.2.

Denote by $P_n = \prod_{i=1}^{n}(i^2+1)$ and $L_n = \operatorname{lcm}(1^2+1, 2^2+1, \dots, n^2+1)$, and write $\alpha_p(n) = \operatorname{ord}_p(P_n)$ and $\beta_p(n) = \operatorname{ord}_p(L_n)$. The argument for estimating L_n stems from the following equality:

$$\log L_n = \log P_n + \sum_p (\beta_p(n) - \alpha_p(n)) \log p.$$

Clearly it is not difficult to estimate $\log P_n$. Indeed, using Stirling's approximation formula,we get

$$\begin{aligned}\log \prod_{i=i}^{n}(i^2+1) &= \log \prod_{i=1}^{n} i^2 + \log \prod_{i=1}^{n}\left(1+\frac{1}{i^2}\right)\\ &= 2\log n! + O(1)\\ &= 2n\log n - 2n + O(\log n),\end{aligned}$$

and so in the remainder of the section we will be concerned with the estimation of $\sum_p(\beta_p(n) - \alpha_p(n))\log p$. We start here by making three simple observations:

Lemma 3.

i) $\beta_2(n) - \alpha_2(n) = -n/2 + O(1)$,

ii) $\beta_p(n) - \alpha_p(n) = 0$, *when* $p > 2n$.

iii) $\beta_p(n) = \alpha_p(n) = 0$, *when* $p \equiv 3 \pmod 4$.

Proof.

i) i^2+1 is never divisible by 4 and is divisible by 2 for every odd i.

ii) Note that $\alpha_p(n) \neq \beta_p(n)$ only if there exist $i < j \leq n$ such that $p|i^2+1$ and $p|j^2+1$. But this implies $p|(i-j)(i+j)$, and so $p \leq 2n$.

iii) i^2+1 is never divisible by $p \equiv 3 \pmod 4$ as -1 is not a quadratic residue modulo such prime.

□

Since we have dealt with the prime 2, from now on we will only consider odd primes. Lemma 3 also states that it is sufficient to study the order of prime numbers which are smaller than $2n$ and are equivalent to 1 modulo 4. We split these primes in two groups: ones that are smaller than $n^{2/3}$ and others that are between $n^{2/3}$ and $2n$, *small* and *medium* primes respectively.

3.1.1 Small primes

The computation for small primes is easy and is carried out in the lemma below, after obtaining simple estimates for $\alpha_p(n)$ and $\beta_p(n)$. Analysis of medium primes, which is left for the next section, is more subtle and will lead to improvement of the error term.

Lemma 4. *For primes $p \equiv 1 \pmod 4$ the following estimates hold:*

i) $\beta_p(n) \ll \dfrac{\log n}{\log p}$,

ii) $\alpha_p(n) = \dfrac{2n}{p-1} + O\left(\dfrac{\log n}{\log p}\right)$.

Proof.

i) It is clear that $\beta_p(n)$ satisfies $p^{\beta_p(n)} \leq n^2+1$, so

$$\beta_p(n) \leq \frac{\log(n^2+1)}{\log p} \ll \frac{\log n}{\log p}.$$

ii) In order to estimate $\alpha_p(n)$ note that for primes $p \equiv 1 \pmod 4$ the equation $i^2 \equiv -1 \pmod{p^a}$ has two solutions ν_1 and ν_2 in the interval $[1, p^a]$ and every other solution is of the form $\nu_1 + kp^a$ or $\nu_2 + kp^a$, $k \in \mathbb{Z}$. The number of times p^a divides i^2+1, $i = 1, \ldots, n$ is given by

$$2 + \left\lfloor \frac{n-\nu_1}{p^a} \right\rfloor + \left\lfloor \frac{n-\nu_2}{p^a} \right\rfloor, \tag{3.5}$$

which equals to 0 for $p^a > n^2+1$ and $2n/p^a + O(1)$ for $p^a \le n^2+1$. Therefore we get

$$\begin{aligned}\alpha_p(n) &= 2\sum_{j=1}^{\left\lfloor \frac{\log(n^2+1)}{\log p}\right\rfloor} \frac{n}{p^j} + O\left(\frac{\log n}{\log p}\right)\\ &= 2n\sum_{j=1}^{\infty}\frac{1}{p^j} - 2n\sum_{j=\left\lfloor \frac{\log(n^2+1)}{\log p}\right\rfloor+1}^{\infty}\frac{1}{p^j} + O\left(\frac{\log n}{\log p}\right)\\ &= \frac{2n}{p-1} + O\left(\frac{\log n}{\log p}\right),\end{aligned}$$

and the claim follows. □

Lemma 5. *The following estimate holds:*

$$\sum_{2<p<n^{2/3}} (\alpha_p(n) - \beta_p(n))\log p = \sum_{2<p<n^{2/3}} \frac{\left(1+\left(\frac{-1}{p}\right)\right) n\log p}{p-1} + O(n^{2/3}).$$

Proof. Using the estimates from Lemma 4 we get

$$\sum_{2<p<n^{2/3}} \beta_p(n)\log p \ll \sum_{2<p<n^{2/3}} \log n \ll n^{2/3},$$

and also

$$\begin{aligned}\sum_{2<p<n^{2/3}} \alpha_p(n)\log p &= \sum_{\substack{p<n^{2/3}\\ p\equiv 1 \pmod 4}} \left(\frac{2n\log p}{p-1} + O(\log n)\right)\\ &= \sum_{2<p<n^{2/3}} \frac{\left(1+\left(\frac{-1}{p}\right)\right) n\log p}{p-1} + O(n^{2/3}),\end{aligned}$$

and hence the claim follows. □

3.1.2 Medium primes

In order to deal with the remaining primes, we note, that if a prime $p \equiv 1 \pmod 4$ satisfies $n^{2/3} \le p \le 2n$ then it divides i^2+1 for some $i \le n$. However, since such a prime is sufficiently large compared to n^2+1, the case that p^2 divides some i^2+1, $i \le n$ is unlikely.

Having this in mind, we separate the contribution of higher degrees from the contribution of degree 1. Define for $p \equiv 1 \pmod 4$:

$$\begin{aligned}\alpha_p^*(n) &= \left|\{i : p|i^2+1,\ i \le n\}\right|,\\ \beta_p^*(n) &= 1,\end{aligned}$$

and, for $p \equiv 3 \pmod 4$, $\alpha_p^*(n) = \beta_p^*(n) = 0$. Then

$$\sum_{n^{2/3}\le p\le 2n} (\beta_p(n)-\alpha_p(n))\log p = \sum_{n^{2/3}\le p\le 2n} \beta_p^*(n)\log p - \sum_{n^{2/3}\le p\le 2n} \alpha_p^*(n)\log p + \sum_{n^{2/3}\le p\le 2n} (\beta_p(n)-\beta_p^*(n)-\alpha_p(n)+\alpha_p^*(n))\log p \tag{3.6}$$

We now estimate each sum in the previous equation. We start estimating the last one:

Lemma 6. *The following estimate holds:*

$$\sum_{n^{2/3}\le p\le 2n} (\beta_p(n)-\beta_p^*(n)-\alpha_p(n)+\alpha_p^*(n))\log p \ll n^{2/3}\log n.$$

To prove this lemma we need some preliminary results. As it was intended, if $(\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n))\log p$ is nonzero, then we must have $p^2|i^2+1$ for some $i \le n$. We claim, that number of such primes is small:

Lemma 7. *The following estimate holds:*

$$\Big|\{p:\ p^2|i^2+1,\ n^{2/3}\le p\le 2n, i\le n\}\Big| \ll n^{2/3}.$$

Proof. Let us split the interval $[n^{2/3}, 2n]$ into dyadic intervals, consider one of them, say $[Q, 2Q]$, and define

$$P_k = \{\, p:\ i^2+1 = kp^2 \ \text{ for some } i\le n\}.$$

We estimate the size of the set $P_k \cap [Q, 2Q]$, which is nonempty only when $k \le (n^2+1)/Q^2$. For every $p \in P_k \cap [Q, 2Q]$ we have $i^2 - kp^2 = (i+\sqrt{k}p)(i-\sqrt{k}p) = -1$, thus

$$\left|\frac{i}{p} - \sqrt{k}\right| = \frac{1}{p^2}\left(\frac{i}{p}+\sqrt{k}\right)^{-1} \le \frac{1}{p^2} \le \frac{1}{Q^2}.$$

On the other hand, all fractions i/p, $p \in P_k$, are pairwise different, since $ip' = i'p$ implies $p = p'$ (otherwise $p|i$ and so $p|i^2 - kp^2 = -1$, a contradiction), therefore

$$\left|\frac{i}{p} - \frac{i'}{p'}\right| \ge \frac{1}{pp'} \gg \frac{1}{Q^2}.$$

Combining both inequalities we get $|P_k \cap [Q, 2Q]| \ll 1$ for every $k \le (n^2+1)/Q^2$. Recalling that $P_k \cap [Q, 2Q]$ is empty for other values of k we have

$$\big|\{p:\ p^2|i^2+1,\ Q\le p\le 2Q,\ i\le n\}\big| = |\cup_k (P_k \cap [Q, 2Q])| \ll \frac{n^2}{Q^2}.$$

Summing over all dyadic intervals the result follows. □

Now we use this estimate to prove Lemma 6.

Proof of Lemma 6. We use estimates from Lemma 4 and the estimate for $\alpha_p^*(n)$, which follows from Expression (3.5):

$$\begin{aligned}\beta_p(n) &\ll \frac{\log n}{\log p},\\ \alpha_p(n) &= \frac{2n}{p-1} + O\left(\frac{\log n}{\log p}\right),\\ \alpha_p^*(n) &= \frac{2n}{p} + O(1).\end{aligned}$$

For any prime $n^{2/3} < p < 2n$, such that $p^2 | i^2 + 1$ for some $i \leq n$, we get

$$\left|\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)\right| = \frac{2n}{p(p-1)} + O\left(\frac{\log n}{\log p}\right) \ll \frac{\log n}{\log p}.$$

It follows from Lemma 7 that the number of such primes is $\ll n^{2/3}$, thus

$$\sum_{n^{2/3} \leq p \leq 2n} (\beta_p(n) - \beta_p^*(n) - \alpha_p(n) + \alpha_p^*(n)) \log p \ll n^{2/3} \log n.$$

□

We continue estimating the second sum in Equation (3.6):

Lemma 8. *The following estimate holds:*

$$\sum_{n^{2/3} \leq p \leq 2n} \beta_p^*(n) \log p = n + O\left(\frac{n}{\log n}\right).$$

Proof. Summing by parts and using estimate (3.4) for $\pi_1(x)$ we get:

$$\begin{aligned}\sum_{n^{2/3} \leq p \leq 2n} \beta_p^*(n) \log p &= \sum_{\substack{n^{2/3} \leq p \leq 2n \\ p \equiv 1 \pmod 4}} \log p\\ &= \sum_{\substack{p \leq 2n \\ p \equiv 1 \pmod 4}} \log p + O(n^{2/3})\\ &= \log(2n)\, \pi_1(2n) - \int_2^{2n} \frac{\pi_1(t)}{t}\, \mathrm{d}t + O(n^{2/3})\\ &= n + O\left(\frac{n}{\log n}\right).\end{aligned}$$

□

Finally, we deal with the contribution of the coefficients α_p^*. In this point we need to take care of the error term in a more detailed way:

Lemma 9. *For any $\epsilon < 8/9$ the following estimate holds:*

$$\sum_{n^{2/3}\le p\le 2n} \alpha_p^*(n)\log p = n\sum_{n^{2/3}\le p\le 2n} \frac{\left(1+\left(\frac{-1}{p}\right)\right)\log p}{p-1} + O\left(\frac{n}{(\log n)^{\epsilon/2}}\right).$$

Proof. Using (3.5) and noting that $\nu_1+\nu_2 = p$, where $1\le \nu_1,\nu_2\le p$ are solutions of $i^2\equiv -1 \pmod p$, we get

$$\begin{aligned}\alpha_p^*(n) &= 2+\left\lfloor\frac{n-\nu_1}{p}\right\rfloor+\left\lfloor\frac{n-\nu_2}{p}\right\rfloor\\ &= 2+\frac{2n}{p}-\frac{\nu_1+\nu_2}{p}-\left\{\frac{n-\nu_1}{p}\right\}-\left\{\frac{n-\nu_2}{p}\right\}\\ &= \frac{2n}{p}+\frac12-\left\{\frac{n-\nu_1}{p}\right\}+\frac12-\left\{\frac{n-\nu_2}{p}\right\},\end{aligned}$$

so the sum over all primes in the interval $[n^{2/3},2n]$ is equal to

$$\begin{aligned}\sum_{n^{2/3}\le p\le 2n}\alpha_p^*(n)\log p = n\sum_{n^{2/3}\le p\le 2n}&\frac{\left(1+\left(\frac{-1}{p}\right)\right)\log p}{p}\\ &+\sum_{\substack{n^{2/3}\le p\le 2n\\ \nu^2\equiv -1\,(p)\\ 0\le\nu<p}}\log p\left(\frac12-\left\{\frac{n-\nu}{p}\right\}\right).\end{aligned}$$

We rewrite

$$n\sum_{n^{2/3}\le p\le 2n}\frac{\left(1+\left(\frac{-1}{p}\right)\right)\log p}{p} = n\sum_{n^{2/3}\le p\le 2n}\frac{\left(1+\left(\frac{-1}{p}\right)\right)\log p}{p-1}+O(n^{1/3}\log n)$$

and

$$\begin{aligned}&\sum_{n^{2/3}\le p\le 2n}\sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)}}\log p\left(\frac12-\left\{\frac{n-\nu}{p}\right\}\right)\\ &\qquad=\log n\sum_{p\le 2n}\sum_{\substack{0<\nu<p\\ \nu^2\equiv -1\,(p)}}\left(\frac12-\left\{\frac{n-\nu}{p}\right\}\right)+O\left(\frac{n}{\log n}\right).\end{aligned}$$

Notice that for any sequence a_p satisfying $a_p\ll 1$ we have by summation by parts argument that

$$\sum_{p<x}a_p\log p = \log x\sum_{p<x}a_p-\int_1^x\frac1t\sum_{p<t}a_p\,\mathrm{d}t = \log x\sum_{p<x}a_p+O\left(\frac{x}{\log x}\right).$$

In order to get the claimed bound, it remains to show that

$$\sum_{p\le 2n}\sum_{\substack{0<\nu<p\\ \nu^2\equiv -1\,(p)}}\left(\frac12-\left\{\frac{n-\nu}{p}\right\}\right)=O\left(\frac{n}{(\log n)^{1+\epsilon/2}}\right).$$

To do that, we divide the summation interval into $1+H$ parts $[1,2n]=[1,A]\cup L_1\cup\cdots\cup L_H$, where

$$L_i=\left(\frac{2nAH}{2n(H-i+1)+A(i-1)},\frac{2nAH}{2n(H-i)+Ai}\right].$$

We choose $A=\lfloor n/(\log n)^{\epsilon/2}\rfloor$ and $H=\lfloor(\log n)^{\epsilon}\rfloor$ in order to minimize the error term, but we continue using these notations for the sake of conciseness.

Observe that in every of these parts, except the first one, n/p is almost constant, which enables to use the fact that ν/p is well distributed. More precisely, if $p\in L_i$ then

$$\frac{n}{p}\in[\lambda_i,\lambda_{i-1}):=\left[\frac{2n(H-i)+Ai}{2AH},\frac{2n(H-i+1)+A(i-1)}{2AH}\right),$$

and the length of such interval is small: $|[\lambda_i,\lambda_{i-1})|=\frac{2n-A}{2AH}$. We would then like to replace $\frac{n}{p}$ by λ_i whenever $\frac{n}{p}\in[\lambda_i,\lambda_{i-1})$ using

$$\left\{\frac{n}{p}-\frac{\nu}{p}\right\}=\left\{\lambda_i-\frac{\nu}{p}\right\}+\left\{\frac{n}{p}-\lambda_i\right\},\tag{3.7}$$

but this equality does not hold if $\lambda_i<\frac{\nu}{p}+k<\frac{n}{p}$ for some integer k, in particular $\frac{\nu}{p}+k\in[\lambda_i,\lambda_{i-1}]$. Therefore we must distinguish these two cases: if $\lambda_i\le\frac{\nu}{p}+k\le\lambda_{i-1}$ for some k we rewrite it as $\frac{\nu}{p}\in[\lambda_i,\lambda_{i-1}]_1$ and $\frac{\nu}{p}\notin[\lambda_i,\lambda_{i-1}]_1$ otherwise.

We now split the previous sum into three parts:

$$\sum_{p\le 2n}\sum_{\substack{0<\nu<p\\ \nu^2\equiv -1\,(p)}}\left(\frac12-\left\{\frac{n-\nu}{p}\right\}\right)=\Sigma_1+\Sigma_2+\Sigma_3+O(\pi_1(A)),$$

where Σ_1, Σ_2 and Σ_3 are defined as

$$\Sigma_1=\sum_{i=1}^{H}\sum_{p\in L_i}\sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)}}\left(\frac12-\left\{\lambda_i-\frac{\nu}{p}\right\}\right),$$

$$\Sigma_2=\sum_{i=1}^{H}\sum_{p\in L_i}\sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)\\ \frac{\nu}{p}\notin[\lambda_i,\lambda_{i-1}]_1}}\left(\left\{\lambda_i-\frac{\nu}{p}\right\}-\left\{\frac{n}{p}-\frac{\nu}{p}\right\}\right),$$

$$\Sigma_3=\sum_{i=1}^{H}\sum_{p\in L_i}\sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)\\ \frac{\nu}{p}\in[\lambda_i,\lambda_{i-1}]_1}}\left(\left\{\lambda_i-\frac{\nu}{p}\right\}-\left\{\frac{n}{p}-\frac{\nu}{p}\right\}\right).$$

Recall that $A=n/(\log n)^{\epsilon/2}+O(1)$ and $H=(\log n)^{\epsilon}+O(1)$, so $\pi_1(A)=O(n/(\log n)^{1+\epsilon/2})$. We now estimate each of the sums $\Sigma_1,\Sigma_2,\Sigma_3$ separately, making use of Lemma 21 (see Appendix refsec:appendix). For the first one note that

$$\int_0^1\left(\frac12-\{\lambda_i-t\}\right)\mathrm{d}t=0,$$

so we get, using Lemma 21,

$$\begin{aligned}\Sigma_1 &= \sum_{i=1}^{H} \sum_{p\in L_i} \sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)}} \left(\frac{1}{2} - \left\{\lambda_i - \frac{\nu}{p}\right\}\right)\\ &= \sum_{i=1}^{H} O\left(\frac{2nAH}{2n(H-i)+Ai} \Big/ \left(\log\tfrac{2nAH}{2n(H-i)+Ai}\right)^{1+\epsilon}\right) \qquad (3.8)\\ &= O\left(\frac{2nAH}{(\log n)^{1+\epsilon}} \int_0^H \frac{\mathrm{d}i}{2n(H-i)+Ai}\right)\\ &= O\left(\frac{2nAH}{(\log n)^{1+\epsilon}} \frac{\log 2n/A}{2n-A}\right) = O\left(\frac{n\log\log n}{(\log n)^{1+\epsilon/2}}\right).\end{aligned}$$

For the second sum we use Equation (3.7):

$$\begin{aligned}\Sigma_2 &= \sum_{i=1}^{H} \sum_{p\in L_i} \sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)\\ \frac{\nu}{p}\notin[\lambda_i,\lambda_{i-1}]_1}} \left\{\frac{n}{p} - \lambda_i\right\}\\ &\le \sum_{i=1}^{H} \sum_{p\in L_i} \sum_{\substack{0\le\nu<p\\ \nu^2\equiv -1\,(p)}} |[\lambda_i,\lambda_{i-1}]| \qquad (3.9)\\ &\le \frac{2n-A}{2AH} 2\pi_1(2n) = O\left(\frac{n}{(\log n)^{1+\epsilon/2}}\right).\end{aligned}$$

Finally, for the third sum we use the notation $\mathbb{I}_{[\lambda_i,\lambda_{i-1}]_1}$ for the indicator function of the interval $[\lambda_i,\lambda_{i-1}]$ modulo 1, which satisfies

$$\int_0^1 \mathbb{I}_{[\lambda_i,\lambda_{i-1}]_1}(t)\,\mathrm{d}t = |[\lambda_i,\lambda_{i-1}]|,$$

so using Lemma 21 we get

$$\begin{aligned}\Sigma_3 &\ll \sum_{i=1}^{H} \sum_{\substack{0\le\nu<p\in L_i\\ \nu^2\equiv -1\,(p)\\ \frac{\nu}{p}\in[\lambda_i,\lambda_{i-1}]_1}} 1 = \sum_{i=1}^{H} \sum_{\substack{0\le\nu<p\in L_i\\ \nu^2\equiv -1\,(p)}} \mathbb{I}_{[\lambda_i,\lambda_{i-1}]_1}\left(\frac{\nu}{p}\right)\\ &= \sum_{i=1}^{H} 2\pi_i(L_i)|[\lambda_i,\lambda_{i-1}]| + O\left(\frac{2nAH}{2n(H-i)+Ai} \Big/ \left(\log\tfrac{2nAH}{2n(H-i)+Ai}\right)^{1+\epsilon}\right).\\ &= O\left(\frac{n\log\log n}{(\log n)^{1+\epsilon/2}}\right),\end{aligned}$$

estimating similarly as in the derivation of (3.8) and (3.9).

Finally, we note that any function f satisfying $f(n) = O\left(\frac{n\log\log n}{(\log n)^{1+\epsilon/2}}\right)$ for every $\epsilon < 8/9$ also satisfies $f(n) = O\left(\frac{n}{(\log n)^{1+\epsilon/2}}\right)$ for every $\epsilon < 8/9$, hence this concludes the proof. □

Let us now conclude the proof of Theorem 15.

Proof of Theorem 15. Combining Lemmas 5, 6, 8 and 9, and taking $\theta = \epsilon/2$, we get that

$$\log L_n = 2n\log n - n\left(1 + \frac{\log 2}{2} + \sum_{2<p\le 2n} \frac{\left(1+\left(\frac{-1}{p}\right)\right)\log p}{p-1}\right) + O\left(\frac{n}{(\log n)^\theta}\right),$$

for any constant $\theta < 4/9$. Note that,

$$\sum_{2<p\le 2n} \frac{\left(1+\left(\frac{-1}{p}\right)\right)\log p}{p-1} = \sum_{2<p\le 2n} \frac{\log p}{p-1} + \sum_{2<p\le 2n} \frac{\left(\frac{-1}{p}\right)\log p}{p-1}.$$

For the first sum, observe that Merten's Theorem implies

$$\sum_{2<p\le 2n} \frac{\log p}{p-1} = \sum_{p^j\le 2n} \frac{\log p}{p^j} - \log 2 + \sum_{\substack{p^j>2n\\ 2<p\le 2n}} \frac{\log p}{p^j} = \log n - \gamma + o(1),$$

and the error term can be bounded by $O\left(1/\log n\right)$ using Prime Number Theorem in the form (3.3) and by summation by parts. Note that this bound can be sharpened to $O(\exp(-c\sqrt{\log n}))$ for certain constant c, see [78] (Exercise 4, page 182).

For the second sum, we recall that the complete oscillating sum is convergent, and it follows from Prime Number Theorem in arithmetic progressions that

$$\sum_{2<p\le 2n} \frac{\left(\frac{-1}{p}\right)\log p}{p-1} = \sum_{p\ne 2} \frac{\left(\frac{-1}{p}\right)\log p}{p-1} + O\left(\frac{1}{\log n}\right).$$

Thus we have that, for every $\theta < 4/9$,

$$\log L_n = n\log n - n\left(1 - \gamma + \frac{\log 2}{2} + \sum_{p\ne 2} \frac{\left(\frac{-1}{p}\right)\log p}{p-1}\right) + O\left(\frac{n}{(\log n)^\theta}\right),$$

which completes the proof.

3.2 Random case: two natural models for random sets

In this section we will study the quantity $\psi(S)$ when S is a randomly chosen subset of $[n]$, considering two different models related to the $\mathcal{G}(n,p)$ and $\mathcal{G}(n,M)$ models in random graphs and obtaining the asymptotic for this quantity in the two cases, which holds almost surely as $n\to\infty$.

In the first model each element in S is chosen independently at random in $\{1,\dots,n\}$ with certain probability $\delta = \delta(n)$, and it is denoted by $B(n,\delta)$. In the second model, $S(n,k)$, one restricts attention to k-subsets of $\{1,\dots,n\}$ (where $k = k(n)$), picking among the $\binom{n}{k}$ possibilities uniformly and at random.

Chebyshev's function for random sets in $B(n,\delta)$

The following lemma provides us with an explicit expression for $\psi(S)$ in terms of the von Mangoldt function

$$\Lambda(m) = \begin{cases} \log p & \text{if } m = p^k \text{ for some } k \geq 1 \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 10. *For any set of positive integers S we have $\psi(S) = \sum_m \Lambda(m) I_S(m)$, where Λ denotes the classical von Mangoldt function and*

$$I_S(m) = \begin{cases} 1 & \text{if } S \cap \{m, 2m, 3m, \dots\} \neq \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We observe that for any positive integer l, the number $\log l$ can be written as $\log l = \sum_{p^k | l} \log p$, where the sum is taken over all the powers of primes. Thus, using that $p^k | \operatorname{lcm}\{a : a \in S\}$ if and only if $S \cap \{p^k, 2p^k, 3p^k, \dots\} \neq \emptyset$, we get

$$\log \operatorname{lcm}\{a : \ a \in S\} = \sum_{p^k | \operatorname{lcm}\{a:\ a \in S\}} \log p = \sum_{p^k} (\log p) I_S(p^k) = \sum_m \Lambda(m) I_S(m).$$

□

Note that if $S = \{1, \dots, n\}$ then $\psi(S) = \sum_{m \leq n} \Lambda(m)$ is the classical Chebychev function $\psi(n)$.

Let us now define the random variable $X = \psi(S)$ where S is a random set in $B(n,\delta)$. With this notation in mind, we have that the expectation and variance are

$$\begin{aligned} \mathbb{E}(X) &= \sum_{m \leq n} \Lambda(m) \mathbb{E}(I_S(m)) \\ V(X) &= \sum_{m,l \leq n} \Lambda(m)\Lambda(l) \left(\mathbb{E}(I_S(m) I_S(l)) - \mathbb{E}\left(I_S(m)\right) \mathbb{E}\left(I_S(l)\right) \right). \end{aligned}$$

Chebyshev's function for random sets in $S(n,k)$

Let us consider again the random variable $X = \psi(S)$, but in the model $S(n,k)$. From now on $\mathbb{E}_k(X)$ and $V_k(X)$ will denote the expected value and the variance of X in this probability space. Clearly, for $s = 1, 2$ we have

$$\begin{aligned} \mathbb{E}_k(X^s) &= \frac{1}{\binom{n}{k}} \sum_{|S|=k} \psi^s(S) \\ V_k(X) &= \frac{1}{\binom{n}{k}} \sum_{|S|=k} \left(\psi(S) - \mathbb{E}_k(X)\right)^2 \end{aligned}$$

We first must study the problem in $B(n,\delta)$ and prove Theorem 17. In Section 3.2.1 we estimate the expectation and variance to show that $\mathbb{V}(X) = o\left(\mathbb{E}(X)^2\right)$ in order to apply Theorem 31. In section 3.2.2 we compare the model $B(n,\delta)$ with $S(n,k)$ to conclude that both models are asymptotically equivalent in this context when $\delta = k/n$. Finally, Section 3.2.3 focuses on the case k constant.

3.2.1 The lcm in $B(n,\delta)$

First of all we give an explicit expression for the expected value of the random variable $X = \psi(S)$ where S is a random set in $B(n,\delta)$.

Proposition 3. *For the random variable $X = \psi(S)$ in $B(n,\delta)$ we have*

$$\mathbb{E}\,(X) = n\frac{\delta\log(\delta^{-1})}{1-\delta} + \delta\sum_{r\geq 1} R\left(\frac{n}{r}\right)(1-\delta)^{r-1},$$

where $R(x) = \psi(x) - x$ denotes the error term in the Prime Number Theorem.

Proof. The ambiguous case $\delta = 1$ must be understood as the limit as $\delta \to 1$, which recovers the equality $\psi(n) = n + R(n)$. In the following we assume that $\delta < 1$. By linearity of the expectation, Lemma 10 clearly implies

$$\mathbb{E}(X) = \sum_{m\leq n}\Lambda(m)\mathbb{E}(I_S(m)).$$

Since $\mathbb{E}(I_S(m)) = \mathbb{P}(S\cap\{m,2m,\dots\}\neq\emptyset) = 1 - \prod_{r\leq n/m}\mathbb{P}(rm\notin S) = 1-(1-\delta)^{\lfloor n/m\rfloor}$, we obtain

$$\mathbb{E}(X) = \sum_{m\leq n}\Lambda(m)\left(1-(1-\delta)^{\lfloor n/m\rfloor}\right). \tag{3.10}$$

We observe that $\lfloor n/m\rfloor = r$ whenever $\frac{n}{r+1} < m \leq \frac{n}{r}$, so we split the sum into intervals $J_r = (\frac{n}{r+1}, \frac{n}{r}]$, obtaining

$$\begin{aligned}
\mathbb{E}\,(X) &= \sum_{r\geq 1}(1-(1-\delta)^r)\sum_{m\in J_r}\Lambda(m)\\
&= \sum_{r\geq 1}(1-(1-\delta)^r)\left(\psi\Big(\frac{n}{r}\Big) - \psi\Big(\frac{n}{r+1}\Big)\right)\\
&= \delta\sum_{r\geq 1}\psi\Big(\frac{n}{r}\Big)(1-\delta)^{r-1}\\
&= \delta n\sum_{r\geq 1}\frac{(1-\delta)^{r-1}}{r} + \delta\sum_{r\geq 1}R\left(\frac{n}{r}\right)(1-\delta)^{r-1}.\\
&= n\frac{\delta\log(\delta^{-1})}{1-\delta} + \delta\sum_{r\geq 1}R\left(\frac{n}{r}\right)(1-\delta)^{r-1}.
\end{aligned}$$

□

Corollary 10. *If $\delta = \delta(n) < 1$ and $\delta n\to\infty$ then*

$$\mathbb{E}\,(X) = n\frac{\delta\log(\delta^{-1})}{1-\delta}\left(1+O\left(e^{-C\sqrt{\log(\delta n)}}\right)\right)$$

for some constant $C > 0$.

Proof. We estimate the absolute value of the sum appearing in Proposition 3. For any positive integer T and using that $|R(y)| < 2y$ for all $y > 0$ we have

$$\begin{aligned}\sum_{r\geq 1} |R(n/r)|(1-\delta)^{r-1} &= \sum_{1\leq r\leq T} |R(n/r)|(1-\delta)^{r-1} + \sum_{r\geq T+1} |R(n/r)|(1-\delta)^{r-1}\\ &\leq n\sum_{1\leq r\leq T} \frac{|R(n/r)|}{(n/r)}\frac{(1-\delta)^{r-1}}{r} + 2n\sum_{r\geq T+1}\frac{(1-\delta)^{r-1}}{r}\\ &\leq n\left(\max_{x\geq n/T}\frac{|R(x)|}{x}\right)\sum_{1\leq r\leq T}\frac{(1-\delta)^{r-1}}{r} + 2n\sum_{r\geq T+1}\frac{(1-\delta)^{r-1}}{r}\\ &\leq n\frac{\log(\delta^{-1})}{(1-\delta)}\left(\max_{x\geq n/T}\frac{|R(x)|}{x}\right) + \frac{2n}{T+1}\frac{(1-\delta)^T}{\delta}\end{aligned}$$

Taking into account that $(1-\delta)^T < e^{-\delta T}$ and the known estimate

$$\max_{x>y}\frac{|R(x)|}{x} \ll e^{-C_1\sqrt{\log y}}$$

for the error term in the Prime Number Theorem, we have

$$\sum_{r\geq 1}|R(n/r)|(1-\delta)^{r-1} \ll n\frac{\log(\delta^{-1})}{(1-\delta)}e^{-C_1\sqrt{\log(n/T)}} + n\frac{e^{-\delta T}}{\delta T}.$$

Thus we have proved that for any positive integer T we have

$$\mathbb{E}(X) = n\frac{\delta\log(\delta^{-1})}{1-\delta}\left(1 + O\left(e^{-C_1\sqrt{\log(n/T)}}\right) + O\left(\frac{1-\delta}{\log(\delta^{-1})}\frac{e^{-\delta T}}{\delta T}\right)\right).$$

We take $T \asymp \delta^{-1}\sqrt{\log(\delta n)}$ to minimize the error term. To estimate the first error term we observe that $\log(n/T) \gg \log(\delta n/\sqrt{\log(\delta n)}) \gg \log(\delta n)$, so for some constant C

$$e^{-C_1\sqrt{\log(n/T)}} \ll e^{-C\sqrt{\log(\delta n)}}.$$

To bound the second error term we simply observe that $\delta T > 1$ and that $\frac{1-\delta}{\log(\delta^{-1})} \leq 1$ and we get a similar upper bound. □

We must now study the variance of the random variable X.

Proposition 4. *For the random variable $X = \psi(S)$ in $B(n,\delta)$ we have*

$$V(X) \ll \delta n\log^2 n.$$

Proof. By linearity of expectation we have that

$$\begin{aligned}V(X) &= \mathbb{E}\left(X^2\right) - \mathbb{E}^2(X)\\ &= \sum_{m,l\leq n}\Lambda(m)\Lambda(l)\left(\mathbb{E}\left(I_S(m)I_S(l)\right) - \mathbb{E}\left(I_S(m)\right)\mathbb{E}\left(I_S(l)\right)\right).\end{aligned}$$

We observe that if $\Lambda(m)\Lambda(l) \neq 0$ then $l \mid m$, $m \mid l$ or $(m,l) = 1$. Let us now study the term $\mathbb{E}(I_S(m)I_S(l))$ in these cases.

(i) If $l \mid m$ then

$$\mathbb{E}(I_S(m)I_S(l)) = 1 - (1-\delta)^{\lfloor n/m \rfloor}.$$

(ii) If $(l,m) = 1$ then

$$\mathbb{E}(I_S(m)I_S(l)) = 1 - (1-\delta)^{\lfloor n/m \rfloor} - (1-\delta)^{\lfloor n/l \rfloor} + (1-\delta)^{\lfloor n/m \rfloor + \lfloor n/l \rfloor - \lfloor n/ml \rfloor}.$$

Both of these relations are subsumed in

$$\mathbb{E}(I_S(m)I_S(l)) = 1 - (1-\delta)^{\lfloor n/m \rfloor} - (1-\delta)^{\lfloor n/l \rfloor} + (1-\delta)^{\lfloor n/m \rfloor + \lfloor n/l \rfloor - \lfloor n(m,l)/ml \rfloor}.$$

Therefore, it follows from (3.10) that for each term in the sum we have

$$\begin{aligned} &\Lambda(m)\Lambda(l)\left(\mathbb{E}\left(I_S(m)I_S(l)\right) - \mathbb{E}\left(I_S(m)\right)\mathbb{E}\left(I_S(l)\right)\right) \\ &= \Lambda(m)\Lambda(l)(1-\delta)^{\lfloor n/m \rfloor + \lfloor n/l \rfloor - \lfloor n(m,l)/ml \rfloor}\left(1 - (1-\delta)^{\lfloor n(m,l)/ml \rfloor}\right). \end{aligned}$$

Finally, by using the inequality $1 - (1-x)^r \leq rx$ we have

$$\Lambda(m)\Lambda(l)\left(\mathbb{E}\left(I_S(m)I_S(l)\right) - \mathbb{E}\left(I_S(m)\right)\mathbb{E}\left(I_S(l)\right)\right) \leq \delta n \frac{\Lambda(l)}{l}\frac{\Lambda(m)}{m}(m,l),$$

and therefore:

$$V(X) \leq 2\delta n \sum_{1 \leq l \leq m \leq n} \frac{\Lambda(l)}{l}\frac{\Lambda(m)}{m}(m,l).$$

We now split the sum according to $l \mid m$ or $(l,m) = 1$ and estimate each one separately.

$$\sum_{\substack{1 \leq l \leq m \leq n \\ l \mid m}} \frac{\Lambda(l)}{l}\frac{\Lambda(m)}{m}(m,l) \leq \sum_{p \leq n}\sum_{1 \leq j \leq i} \frac{\log p}{p^j}\frac{\log p}{p^i}p^j = \sum_{p \leq n}\sum_{1 \leq i} \frac{i \log^2 p}{p^i} \ll \log^2 n,$$

$$\sum_{\substack{1 \leq l \leq m \leq n \\ (l,m)=1}} \frac{\Lambda(l)}{l}\frac{\Lambda(m)}{m}(m,l) \leq \left(\sum_{1 \leq l \leq n} \frac{\Lambda(l)}{l}\right)\left(\sum_{1 \leq m \leq n} \frac{\Lambda(m)}{m}\right) \ll \log^2 n,$$

as we wanted to prove. □

We finish the proof of Theorem 17 by observing that $V(X) = o(\mathbb{E}(X)^2)$ when $\delta n \to \infty$, so $X \sim \mathbb{E}(X)$ asymptotically almost surely.

3.2.2 The lcm in $S(n,k)$

We are now ready to compare the model $S(n,k)$ with the previous model and show that, asymptotically, they are equivalent in this context.

Lemma 11. *For $s = 1, 2$ and $1 \leq j < k$ we have that*

$$\mathbb{E}_j(X^s) \leq \mathbb{E}_k(X^s) \leq \mathbb{E}_j(X^s) + (k^s - j^s)\log^s n.$$

Proof. In order to prove the lower bound it is enough to consider the case $j = k-1$. Observe that the function ψ is monotone with respect to inclusion, i.e. $\psi(S \cup \{a\}) \geq \psi(S)$ for any $S, \{a\} \subseteq [n]$. Using this we get

$$\sum_{|A|=k-1} \psi^s(S) \leq \frac{1}{n-k+1} \sum_{a \in [n]\setminus A} \psi^s(S \cup \{a\}) = \frac{k}{(n-k+1)} \sum_{|A'|=k} \psi^s(S').$$

Inequality then follows from $\binom{n}{k-1} = \frac{k}{(n-k+1)}\binom{n}{k}$.

For the second inequality we observe that for any set $S \in \binom{[n]}{k}$ and any partition into two sets $S = S' \cup S''$ with $|S'| = j$, $|S''| = k-j$ we have that $\psi(S) \leq \psi(S') + \psi(S'') \leq \psi(S') + (k-j)\log n$. Similarly,

$$\begin{aligned}
\psi^2(S) &\leq (\psi(S') + (k-j)\log n)^2 \\
&= \psi^2(S') + 2\psi(S')(k-j)\log n + (k-j)^2 \log^2 n \\
&\leq \psi^2(S') + 2j(k-j)\log^2 n + (k-j)^2 \log^2 n \\
&= \psi^2(S') + (k^2 - j^2)\log^2 n.
\end{aligned}$$

Thus, for $s = 1, 2$ we have

$$\begin{aligned}
\psi^s(S) &\leq \binom{k}{j}^{-1} \sum_{\substack{S' \subset S \\ |S'|=j}} \left(\psi^s(S') + (k^s - j^s)\log^s n\right) \\
&\leq \binom{k}{j}^{-1} \sum_{\substack{S' \subset S \\ |S'|=j}} \psi^s(S') \; + (k^s - j^s)\log^s n.
\end{aligned}$$

Then,

$$\begin{aligned}
\sum_{|S|=k} \psi^s(S) &\leq \binom{k}{j}^{-1} \sum_{|S|=k} \sum_{\substack{S' \subset S \\ |S'|=j}} \psi^s(S') + \binom{n}{k}(k^s - j^s)\log^s n \\
&= \binom{k}{j}^{-1} \sum_{|S'|=j} \psi^s(S') \sum_{\substack{S' \subset S \\ |S|=k}} 1 + \binom{n}{k}(k^s - j^s)\log^s n \\
&= \binom{k}{j}^{-1} \binom{n-j}{k-j} \sum_{|S'|=j} \psi^s(S') + \binom{n}{k}(k^s - j^s)\log^s n \\
&= \frac{\binom{n}{k}}{\binom{n}{j}} \sum_{|S'|=j} \psi^s(S') + \binom{n}{k}(k^s - j^s)\log^s n,
\end{aligned}$$

and the second inequality holds. □

Proposition 5. *For $s = 1, 2$ we have that*

$$\mathbb{E}_k(X^s) = \mathbb{E}(X^s) + O(k^{s-1/2}\log^s n)$$

where $\mathbb{E}(X^s)$ denotes the expectation of X^s in $B(n, k/n)$ and $\mathbb{E}_k(X^s)$ the expectation in $S(n,k)$.

Proof. Observe that for $s = 1, 2$ we have

$$\begin{aligned}\mathbb{E}(X^s) - \mathbb{E}_k(X^s) &= -\mathbb{E}_k(X^s) + \sum_{j=0}^{n} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \sum_{|S|=j} \psi^s(S) \\ &= -\mathbb{E}_k(X^s) + \sum_{j=0}^{n} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} \mathbb{E}_j(X^s) \\ &= \sum_{j=0}^{n} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} \left(\mathbb{E}_j(X^s) - \mathbb{E}_k(X^s)\right),\end{aligned}$$

for $s = 1, 2$. Using Lemma 11 we get

$$|\mathbb{E}_k(X^s) - \mathbb{E}(X^s)| \le \log^s n \sum_{j=0}^{n} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} |j^s - k^s|. \tag{3.11}$$

The sum in (3.11) for $s = 1$ is $\mathbb{E}(|Y - \mathbb{E}(Y)|)$, where $Y \sim \mathrm{Bin}(n, k/n)$ is the binomial distribution of parameters n and k/n. Cauchy–Schwarz inequality for the expectation implies that this quantity is bounded by the standard deviation of the binomial distribution.

$$\sum_{j=0}^{n} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} |j-k| \le \sqrt{n(k/n)(1-k/n)} \le \sqrt{k}, \tag{3.12}$$

which proves Proposition 5 for $s = 1$.

To estimate the sum in (3.11) for $s = 2$, we split the expression in two terms: the sum indexed by $j \le 2k$ and the one with $j > 2k$. We use (3.12) to get

$$\begin{aligned}\sum_{j\le 2k} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} |j^2 - k^2| &\le 3k \sum_{j=0}^{n} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} |j-k| \\ &\le 3k^{3/2}.\end{aligned}$$

On the other hand,

$$\begin{aligned}&\sum_{j>2k} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} |j^2 - k^2| \\ &\le \sum_{l\ge 2} (l+1)^2 k^2 \sum_{lk<j\le(l+1)k} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} \\ &\le \sum_{l\ge 2} (l+1)^2 k^2 \ \mathbb{P}(Y > lk)\end{aligned}$$

where, once again, $Y \sim \mathrm{Bin}(n, k/n)$. Chernoff's inequality (see Lemma 27) implies that for any $\epsilon > 0$ we have

$$\mathbb{P}(Y > (1+\epsilon)k) \le e^{-\epsilon^2 k/3}.$$

Applying this inequality to $\mathbb{P}(Y > lk)$ we get

$$\begin{aligned}&\sum_{j>2k} \left(\frac{k}{n}\right)^j \left(1-\frac{k}{n}\right)^{n-j} \binom{n}{j} |j^2 - k^2| \\ &\le \sum_{l\ge 2} (l+1)^2 k^2 e^{-(l-1)^2 k/3} \ll k^2 e^{-k/3} \ll k^{3/2}.\end{aligned}$$

□

The next corollary proves the first part of Theorem 16.

Corollary 11. *If $k = k(n) < n$ and $k \to \infty$ then*

$$\mathbb{E}_k(X) = k\frac{\log(n/k)}{1-k/n}\left(1 + O\left(e^{-C\sqrt{\log k}}\right)\right)$$

Proof. Proposition 5 for $s = 1$ and Corollary 10 imply that

$$\mathbb{E}_k(X) = k\frac{\log(n/k)}{1-k/n}\left(1 + O\left(e^{-C\sqrt{\log k}}\right) + O\left(k^{-1/2}\log n\frac{1-k/n}{\log(n/k)}\right)\right).$$

It is clear that

$$k^{-1/2}\log n\frac{1-k/n}{\log(n/k)} = O\left(k^{-1/2}\log k\right) = o\left(e^{-C\sqrt{\log k}}\right),$$

when $k \to \infty$, which concludes the proof. □

To conclude the proof of Theorem 16 we combine Proposition 4 and Proposition 5 to estimate the variance $V_k(X)$ in $S(n,k)$:

$$\begin{aligned} V_k(X) &= \mathbb{E}_k(X^2) - \mathbb{E}_k^2(X) \\ &= V(X) + \left(\mathbb{E}_k(X^2) - \mathbb{E}(X^2)\right) + \left(\mathbb{E}(X) - \mathbb{E}_k(X)\right)\left(\mathbb{E}(X) + \mathbb{E}_k(X)\right) \\ &\ll k\log^2 n + \left(k^{1/2}\log n\right)(k\log n) \\ &\ll k^{3/2}\log^2 n. \end{aligned}$$

The second assertion of Theorem 16 is a consequence of the estimate $V_k(X) = o\left(\mathbb{E}_k^2(X)\right)$ when $k \to \infty$.

3.2.3 The case when k is constant

The case when k is constant and $n \to \infty$ is not relevant for our original motivation but we give a brief analysis for the sake of completeness. In this case Fernández and Fernández [42] have proved that $\mathbb{E}_k(\psi(A)) = k\log n + C_k + o(1)$, where

$$C_k = -k + \sum_{j=2}^{k}\binom{k}{j}(-1)^j\frac{\zeta'(j)}{\zeta(j)}.$$

Actually, they consider the probabilistic model with k independent choices in $\{1,\dots,n\}$, but when k is fixed it does not make big differences because the probability of a repetition between the k choices is tiny.

It is easy to prove that with probability $1 - o(1)$ we have that $\psi(A) \sim k\log n$. To see this we observe that

$$a_1\cdots a_k\prod_{i<j}(a_i,a_j)^{-1} \le \operatorname{lcm}(a_1,\dots,a_k) \le a_1\cdots a_k \le n^k,$$

so $\sum_{i=1}^{k}\log a_i - \sum_{i<j}\log(a_i,a_j) \le \psi(A) \le k\log n$.

Now, let us note that $\mathbb{P}(a_i \leq n/\log n \text{ for some } i = 1, \dots, k) \leq k/\log n$ and that $\mathbb{P}((a_i, a_j) \geq \log n) \leq \sum_{d > \log n} \mathbb{P}(d \mid a_i,\ d \mid a_j) \leq \sum_{d>\log n} \frac{1}{d^2} < \frac{1}{\log n}$. These observations imply that with probability at least $1 - \frac{k+2\binom{k}{2}}{\log n} = 1 - \frac{2k}{\log n}$ we have that

$$k \log n \left(1 - O\left(\log\log n/\log n\right)\right) \leq \psi(A) \leq k \log n.$$

The analysis in the model $B(n, \delta)$ when $\delta n \to c$ can be done using again Proposition 3.

$$\mathbb{E}\left(\psi(A)\right) = n\frac{\delta \log(\delta^{-1})}{1-\delta} + \delta \sum_{r < n/\log n} R\left(\frac{n}{r}\right)(1-\delta)^{r-1} + \delta \sum_{n/\log n \leq r \leq n} R\left(\frac{n}{r}\right)(1-\delta)^{r-1}$$

We use the estimate $R(x) \ll x/\log x$ in the first sum and the estimate $R(x) \ll x$ in the second one. We have

$$\begin{aligned}
\mathbb{E}\left(\psi(A)\right) &= c \log n(1 + o(1)) \\
&\quad + O\left(\frac{c}{\log\log n} \sum_{r < \frac{n}{\log n}} \frac{(1-\delta)^{r-1}}{r}\right) + O\left(c \sum_{\frac{n}{\log n} \leq r \leq n} \frac{(1-\delta)^{r-1}}{r}\right) \\
&= c \log n + O\left(\frac{c \log \delta}{\log\log n}\right) + O\left(c \log\log n\right) \\
&= c \log n(1 + o(1)).
\end{aligned}$$

Of course in this model we cannot expect concentration around the expectation because for example the probability that A is the empty set tends to a positive constant, $\mathbb{P}(A = \emptyset) \to e^{-c}$, and then $\mathbb{P}(\psi(A) = 0) \to e^{-c}$.

3.3 The extremal case

In this chapter we have discussed about the quantity $\psi(S)$ and calculate, by means of very different approaches, its asymptotic for different sets of integers.

The underlying question we were trying to answer here is: how close are random sets, arithmetically speaking, from structured ones? Of course this is a very vague statement, so I dedicate this section to develop this idea and conclude it with the (partial) answer we are able to give to it by means of the presented results.

In first place, since we want to compare asymptotics we should fix the range for the elements of our sets: that is $S \subseteq [n]$. Corollary 9 shows that if we choose uniformly at random a subset of $[n]$ then, with probability tending to one as n grows, the least common multiple of this set will be *close* to 2^n, but at this point it is natural to compare sets with the same cardinality, namely $|S| = k + O(1)$ for $k = k(n)$ a given function, since obviously sets with a greater number of elements are more likely to have a higher arithmetical contribution to the lcm.

Observe that, if we focus on the sets $S_1 = \{k^2 + 1 : k = 1, 2, \dots\} \cap [n]$ and $S_2 = \{k^2 - 1 : k = 1, 2, \dots\} \cap [n]$, Theorem 15 states that $\psi(S_1) = \frac{1}{2} n^{1/2} \log n + B n^{1/2} + O\left(\frac{n^{1/2}}{(\log n)^\theta}\right)$ and we know [20] that $\psi(S_2) \sim n^{1/2}$ whereas both sets have cardinality $n^{1/2} + O(1)$. On the other

hand, by Theorem 16 we know that for most sets S in $[n]$ of cardinality $n^{1/2}+O(1)$ we have $\psi(S)=\frac{1}{2}n^{1/2}\log n+o(n^{1/2})$.

Although the asymptotics for $\psi(S_1)$ coincides to the one of a random set of the same size, there are some differences in the second term. Therefore we can conclude that sets arising from polynomials are not typical cases and their difference from the expected value depends on the irreducibility of the polynomial.

Clearly, since we have no deterministic results for sets arising from irreducible polynomials of degree $d\geq 3$ we cannot compare it with the results from Section 3.2. Nevertheless, if we assume Conjecture 1 to be true then, once again, we would have that irreducible polynomials would be closer to behave like typical sets in this sense than reducible ones.

What we still do not know is how far from the expected value $\mathbb{E}(\psi(S))$ the exceptional cases could be. I will finish the discussion in this chapter by including some (partial) results regarding the extremal cases in sets of prescribed size.

Proposition 6. *Let $k=k(n)$ be a function, with $0<k(n)<n$ and $\lim_{n\to\infty}k=\infty$, then*

$$\max_{\substack{S\subseteq[n]\\|S|=k}}\psi(S)\sim\min\{n,k\log n\}.$$

Proof. Let $S\subseteq[n]$ and $|S|=k$. It is clear that

$$\psi(S)\leq\sum_{a\in S}\log a\leq|S|\log n\leq k\log n.$$

On the other hand, it is clear that we always have $\psi(S)\leq\psi(n)\sim n$.

For the lower bound we distinguish two separate cases:

- If $k\geq\left(1-\frac{1}{\log n}\right)\pi(n)$, then we consider any set S of k elements containing the largest $\left(1-\frac{1}{\log n}\right)\pi(n)$ primes in $[n]$ and get

$$\psi(S)\geq\sum_{p\in S}\log p\geq\left(1-\frac{1}{\log n}\right)\sum_{p\leq n}\log p\geq n(1+o(1)).$$

- If $k<\left(1-\frac{1}{\log n}\right)\pi(n)$, then we consider the set S of the k largest primes in $[n]$ and get (denoting the i-th prime by p_i)

$$\psi(S)=\sum_{p\in S}\log p\geq k\log p_{\pi(n)-k}\geq k\log p_{\pi(n)/\log n}\geq k\log n(1+o(1)).$$

□

Proposition 7. *Let $k=k(n)$ be a function with $0<k(n)<n$ and $\lim_{n\to\infty}k=\infty$, then*

$$\min_{\substack{S\subseteq[n]\\|S|=k}}\psi(S)\leq(\log n)^{1+\frac{1}{1-\log k/\log n}+o(1)}.$$

Proof. Let $\Psi(x;B)$ be the number of B-smooth numbers, *i.e.* none of their prime factors is greater than B, less than or equal to x. Canfeld, Erdős and Pomerance [12] proved that for any $\epsilon > 0$ we have

$$\Psi(x;B) = \frac{x}{u^{u+o(u)}},$$

where $u = \log x/\log B$ and $B \leq (\log x)^{1+\epsilon}$. As a consequence of this result, we have

$$\Psi(x;\log^t x) = x^{1-1/t+o(1)} \tag{3.13}$$

for any positive t.

Let T be a real number satisfying $\Psi(n;\log^T n) = k$. By equation (3.13) it is clear that $T = \frac{1}{1-\log k/\log n} + o(1)$. For such T, consider the set S of $\log^T n$-smooth integers $\leq n$, namely

$$S = \{m \leq n \,:\, p|m \Leftarrow p \leq \log^T n\}.$$

Thus

$$\psi(S) = \sum_{p\leq \log^T n} \log p\lfloor \log n/\log p\rfloor \leq \sum_{p\leq \log^T n} \log n \leq (\log n)^{1+\frac{1}{1-\log k/\log n}+o(1)}.$$

□

Chapter 4

Sum of digits of some sequences of integers

For a positive integer $b \geq 2$ let us denote by $s_b(m)$ the sum of the digits of the positive integer m when written in base b. When m runs over a sequence with some combinatorial meaning it is an interesting problem to understand how this quantity behaves with respect to a generic base b, at least for most elements on the sequence. In particular, lower bounds for $s_b(a_n)$ have been investigated before for specific examples of combinatorial sequences $S = \{a_n\}_{n=1}^{\infty}$.

For example, it follows from a result of Stewart [93] (see also [68] for a slightly more general result), that in the case of Fibonacci numbers the inequality

$$s_b(F_n) > c_1 \frac{\log n}{\log \log n}$$

holds for all $n \geq 3$ for some positive constant $c_1 := c_1(b)$ depending on b. In [69] Luca proved the following inequality for the factorial sequence:

$$s_b(n!) > c_2 \log n$$

holds for all $n \geq 1$, where $c_2 := c_2(b)$ is some positive constant depending on b.

Another good example are the lower bounds obtained by Luca and Shparlinski [72] for the sequences of Catalan numbers and middle binomial coefficients, that is $C_n := \frac{1}{n+1}\binom{2n}{n}$ and $D_n := \binom{2n}{n}$ respectively. They show that both inequalities

$$s_b(C_n) > \varepsilon(n)\sqrt{\log n} \qquad \text{and} \qquad s_b(D_n) \geq \varepsilon(n)\sqrt{\log n} \tag{4.1}$$

hold on a set of n of asymptotic density equal to 1, where $\varepsilon(n)$ is any function tending to zero when n tends to infinity. In [71] they also proved that there is some positive constant $c_3 := c_3(b)$ depending on b such that if we denote by

$$A_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$$

the nth Apéry number, then the inequality

$$s_b(A_n) > c_3 \left(\frac{\log n}{\log \log n} \right)^{1/4} \tag{4.2}$$

holds on a set of asymptotic density 1.

Some of the above results were superseded by the results from the recent paper of Knopfmacher and Luca [63], where it is shown that if $\mathbf{r} := (r_0, r_1, \ldots, r_m)$ is a fixed vector of non-negative integers integers with $r_0 > 0$ and

$$S_n(\mathbf{r}) := \sum_{k=0}^{n} \binom{n}{k}^{r_0} \binom{n+k}{k}^{r_1} \cdots \binom{n+km}{k}^{r_m} \quad \text{for} \quad n = 0, 1, \ldots,$$

then for $\mathbf{r} \neq (1)$ there exists a positive constant $c_4 := c_4(b, \mathbf{r})$ depending on both b and $\mathbf{r}$ such that the inequality

$$s_b\left(S_n(\mathbf{r})\right) > c_4 \frac{\log n}{\log \log n} \tag{4.3}$$

holds for almost all n. Note that inequality (4.3) improves (4.1) for the case of the middle binomial coefficients since for $\mathbf{r} = (2)$ we have $S_n(\mathbf{r}) = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n} = D_n$, as well as inequality (4.2) for the case of the Apéry numbers A_n because $A_n = S_n(\mathbf{r})$ for $\mathbf{r} = (2, 2)$.

Note that the case $\mathbf{r} = (1)$ coincides with $S_n(\mathbf{r}) = 2^n$. In this case either b is a power of 2 and $s_b(2^n) = O(1)$ or, when b is not a power of 2, it follows from a result of [93] that $s_b\left(2^n\right) > c_5 \log n / \log \log n$ holds for all sufficiently large positive integers n with some positive constant c_5 depending on b.

In [70], it is shown that if P_n is the partition function of n, which counts the number of distinct ways of representing n as a sum of natural numbers, then the inequality

$$s_b(P_n) > \frac{\log n}{7 \log \log n}$$

holds for almost all positive integers n.

The proofs of such results use a variety of methods from number theory, such as elementary methods, sieve methods, linear forms in logarithms and the subspace theorem of Evertse–Schlickewei–Schmidt [41].

The results discussed in this chapter are included in [25]. In such work we focused on sequences $\{a_n\}_{n=1}^{\infty}$ of positive integers with a certain growth, and show, independently of the combinatorial properties of the sequence, that $s_b(a_n) > c_b \log n$ for almost every element in the sequence, where c_b is a positive number depending both on b as well as on the sequence $\{a_n\}_{n=1}^{\infty}$. In particular, we concentrate on sequences satisfying the asymptotic behavior

$$a_n = e^{f(n)} \left(1 + O\left(n^{-\alpha}\right)\right), \ \alpha > 0,$$

where $f(x)$ is a two times differentiable function satisfying $f''(x) \asymp \frac{1}{x}$ for large x. Many sequences arising in number theory and combinatorics fit into this scheme. The most basic

one, the number of permutations of a set of n elements is clearly a sequence of this kind, since from Stirling's approximation formula we have

$$n! = e^{n\log n - n + \log n + \frac{1}{2}\log 2\pi}\left(1 + O\left(n^{-1}\right)\right). \tag{4.4}$$

The sequence $a_n = \prod_{k=1}^{n}(k^2+1)$ also has similar behavior: $a_n = c_6 n!^2(1+O(n^{-1}))$.

Other interesting sequences arising from combinatorics have more involved expressions, but they also fit into these hypothesis (see [43] for further details). Examples of them are the Bell numbers (that count the number of partitions of sets), involutions (that count the number of permutations of n elements with either fixed points or cycles of length 2) and fragmented permutations (namely, unordered collections of permutations; in other words, *fragments* are obtained by breaking a permutation into pieces).

In graph enumeration, many important families also follow these asymptotic expressions: the number of labelled trees (Cayley trees) with n vertices is equal to n^{n-1}. More generally, it is shown in [43] that families of labelled trees with degree constraints satisfy asymptotic formulas of the form

$$c_{\mathcal{T}} n^{-3/2}\gamma_{\mathcal{T}}^{n}\cdot n!\left(1+O(n^{-1})\right) = e^{f_{\mathcal{T}}(n)}\left(1+O(n^{-1})\right),$$

where the subindex $\mathcal{T}$ indicates the considered constraint and the function $f_{\mathcal{T}}$ is given by

$$f_{\mathcal{T}}(n) = n\log n - n - \log n + n\log\gamma_{\mathcal{T}} + \log c_{\mathcal{T}} + \frac{1}{2}\log 2\pi.$$

Very recently, many authors have shown that several families of labelled graphs satisfies similar formulas: Giménez and Noy [50] (see also [51]) proved that the number of labelled planar graphs with n vertices follows an asymptotic formula of the form

$$c_0 n^{-7/2}\gamma^n\cdot n!\left(1+O\left(n^{-1}\right)\right),$$

where $\gamma \simeq 27.22687$. More generally, as it is shown in [17] (see also [4]), the number of labelled graphs which can be embedded in a surface of genus g satisfies a very similar formula (with the same growth factor). See Table 4.1 for the asymptotics of these sequences.

Sequence	Asymptotic
Permutations	$n!$
$\prod_{k=1}^{n}(k^2+1)$	$cn!^2\left(1+O(n^{-1})\right)$
Involutions	$\frac{1}{2\sqrt{\pi}}n^{-1/2}e^{n/2-1/4}n^{-n/2}\cdot n!\left(1+O\left(n^{-1/5}\right)\right)$
Bell numbers	$\frac{e^{e^r-1}}{r^n\sqrt{2\pi r(r+1)e^r}}\cdot n!\left(1+O\left(e^{-r/5}\right)\right),\ re^r = n+1$
Fragmented permutations	$\frac{1}{2\sqrt{\pi}}n^{-3/4}e^{-1/2+2\sqrt{n}}\cdot n!\left(1+O\left(n^{-3/4}\right)\right)$
Cayley trees	$\frac{1}{\sqrt{2\pi}}n^{-3/2}e^{n}\cdot n!\left(1+O\left(n^{-1}\right)\right)$
Labelled trees	$c_{\mathcal{T}}n^{-3/2}\gamma_{\mathcal{T}}^{n}\cdot n!\left(1+O\left(n^{-1}\right)\right)$
Graphs on surfaces	$c_g n^{5(g-1)/2-1}\gamma^n\cdot n!\left(1+O\left(n^{-1}\right)\right)$

Table 4.1: Combinatorial families and their enumerative asymptotic behavior.

Our main result gives a lower bound for $s_b(a_n)$ for sequences of controlled growth described before.

Theorem 18. *Let $\{a_n\}_{n=1}^{\infty}$ be a sequence of positive integers with asymptotic behavior*

$$a_n = e^{f(n)}\left(1 + O(n^{-\alpha})\right), \text{ with } f''(x) \asymp \frac{1}{x}, \tag{4.5}$$

for some $\alpha > 0$. For any base $b \geq 2$, the inequality

$$s_b(a_n) > \frac{\beta \log n}{10 \log b}, \ \beta = \min\left\{\alpha, \frac{2}{3}\right\}$$

holds on a set of positive integers n of asymptotic density 1.

Proof of Theorem 18. Consider the following set of positive integers:

$$\mathcal{N}_b(x) := \left\{n \in [x/2, x) : s_b(a_n) < \frac{\beta \log n}{10 \log b}\right\},$$

where $\beta \leq \alpha$ will be chosen later. We need to show that $\#\mathcal{N}_b(x) = o(x)$ as $x \to \infty$, since afterwards the conclusion of Theorem 18 will follow by replacing x by $x/2$, then by $x/4$, and so on, and summing up the resulting estimates.

For $n \in \mathcal{N}_b(x)$, we write

$$a_n = d_{k_1} b^{k_1} + d_{k_2} b^{k_2} + \cdots + d_{k_s} b^{k_s}, \tag{4.6}$$

where $d_{k_1}, \ldots, d_{k_s} \in \{1, \ldots, b-1\}$ and $k_1 > k_2 > \cdots > k_s$. Observe that for $i = 1, \ldots, s$ we have

$$a_n = d_{k_1} b^{k_1} + \cdots + d_{k_i} b^{k_i}\left(1 + E_i(n)\right),$$

where $E_i(n) = 0$, if $i = s$, and

$$E_i(n) = \frac{d_{k_{i+1}} b^{k_{i+1}} + \cdots + d_{k_s} b^{k_s}}{d_{k_1} b^{k_1} + \cdots + d_{k_i} b^{k_i}} = O\left(b^{k_{i+1} - k_1}\right),$$

if $i < s$. We choose $k(n)$ to be the smallest k_i such that $b^{k_i - k_1} > n^{-\beta}$.

From the definition of $k(n)$, we immediately see that

$$a_n = \left(d_{k_1} b^{k_1} + \cdots + d_{k(n)} b^{k(n)}\right)\left(1 + O\left(n^{-\beta}\right)\right) = b^{k(n)} D(n)\left(1 + O\left(n^{-\beta}\right)\right), \tag{4.7}$$

where $D(n) = d_{k_1} b^{k_1 - k(n)} + d_{k_2} b^{k_2 - k(n)} + \cdots + d_{k(n)}$.

Let $\mathcal{D}_b(x)$ be the subset of all possible values for $D(n)$, $n \in \mathcal{N}_b(x)$. Let us find an upper bound for the cardinality of this set. First observe that

$$D(n) < b^{k_1 - k(n) + 1} \leq b^{(\beta \log n / \log b) + 1}.$$

The positive integers $D := D(n)$ bounded by the right hand side of the above inequality have at most $K := \lfloor (\beta \log x / \log b) + 2 \rfloor$ digits in base b. As $n \in \mathcal{N}_b(x)$, the number of nonzero digits of $D(n)$ is bounded by $S := \lfloor (\beta \log x / 10 \log b) \rfloor$, and

$$\begin{aligned}
\#\mathcal{D}_b(x) &\leq \sum_{i=0}^{S} \binom{K}{i} (b-1)^i \leq (S+1)\binom{K}{S}(b-1)^S \leq (S+1)\left(\frac{(b-1)eK}{S}\right)^S \\
&\leq \left(\frac{\beta \log x}{10 \log b} + 1\right)\left(10e(b-1) + o(1)\right)^{\frac{\beta \log x}{10 \log b}} = x^{\delta + o(1)}
\end{aligned}$$

as $x \to \infty$, where

$$\delta := \frac{\beta \log(10e(b-1))}{10 \log b}.$$

It can be checked that $\delta < \beta/2$ for all integers $b \geq 2$. Thus, we get that

$$\#\mathcal{D}_b(x) \leq x^{\delta + o(1)} \qquad \text{as} \qquad x \to \infty. \tag{4.8}$$

Combining the fact that $a_n = e^{f(n)}\,(1 + O(n^{-\alpha}))$ with relations (4.6) and (4.7) we have

$$e^{f(n)} = b^{k(n)} D(n) \left(1 + O\left(x^{-\beta}\right)\right),$$

since $n \in [x/2, x)$ and $\beta \leq \alpha$ by hypothesis. Taking logarithms, we get that

$$f(n) = k(n) \log b + \log D(n) + O\left(x^{-\beta}\right). \tag{4.9}$$

We now write

$$\mathcal{N}_b(x) = \bigcup_{D \in \mathcal{D}_b(x)} \mathcal{N}_{b,D}(x),$$

where

$$\mathcal{N}_{b,D}(x) := \{n \in \mathcal{N}_b(x) : D(n) = D\}.$$

Observe that, with this notation, we have

$$\#\mathcal{N}_b(x) \leq \#\mathcal{D}_b(x) \max_{D \in \mathcal{D}_b} \#\mathcal{N}_{b,D}(x),$$

and we must now bound the number of elements lying in each $\mathcal{N}_{b,D}(x)$.

For a fixed $D \in \mathcal{D}_b(x)$ and y depending on x, to be chosen later, we take a look at the elements $n \in \mathcal{N}_{b,D}(x)$. We say that n is *separated* if $[n, n+y] \cap \mathcal{N}_{b,D}(x) = \{n\}$. It is clear that there are at most $x/2y + 1$ elements on $\mathcal{N}_{b,D}(x)$ which are separated.

Let us now count the non-separated elements $n \in \mathcal{N}_{b,D}(x)$. For such an n, there exists $1 \leq m \leq y$ with $n + m \in \mathcal{N}_{b,D}(x)$. Taking the difference of the relations (4.9) in n, $n + m \in \mathcal{N}_{b,D}(x)$ we get

$$\begin{aligned}(k(n+m) - k(n)) \log b &= (f(n+m) - f(n)) + O(x^{-\beta}) \\ &= m f'(\zeta) + O(x^{-\beta}),\end{aligned}$$

where $\zeta \in [n, n+m]$ is some point whose existence is guaranteed by the Intermediate Value Theorem. It follows from condition (4.5), which in particular implies $f'(x) \asymp \log x$, that $k(n+m) \neq k(n)$ for large x (as $x/2 < n < x$) in the above estimate. Thus, non-separated elements n in $\mathcal{N}_{b,D}(x)$ are characterized by their values $k(n)$. Denoting by $\|x\|$ the closest integer to x, for a fixed $m \leq y$, the differences

$$k(m+n) - k(n) = \left\| \frac{m f'(\zeta)}{\log b} \right\| \tag{4.10}$$

take $O(m)$ integer values, since for two elements $n, n+\ell \in \mathcal{N}_{b,D}(x)$ we have by condition (4.5)

$$\frac{m}{\log b} \left(f'(\zeta_{n+\ell}) - f'(\zeta_n)\right) \asymp \frac{m\ell}{x \log b} = O(m).$$

For a fixed difference in (4.10), say M, we must be able to count the number elements $n \in \mathcal{N}_{b,D}(x)$ such that

$$k(n+m) - k(n) = M + O(n^{-\beta}),$$

but it follows from the previous argument that

$$\frac{m}{\log b}\left(f'(\zeta_{n+\ell}) - f'(\zeta_n)\right) = O(x^{-\beta})$$

for at most $O(1+x^{1-\beta}/m)$ values of n. Thus, there are $O(y^2 + yx^{1-\beta})$ non-separated elements in $\mathcal{N}_{b,D}(x)$, for an arbitrary $D \in \mathcal{D}_b(x)$. Setting $y := x^{\beta/2}$, we observe that

$$\#\mathcal{N}_{b,D}(x) \ll yx^{1-\beta} + y^2 + \frac{x}{y} + 1 \ll x^{1-\beta/2} + x^{\beta} \ll x^{1-\beta/2},$$

whenever $\beta \leq 2/3$. Thus, if we choose $\beta := \min\{\alpha, 2/3\}$ it follows from estimate (4.8) that

$$\#\mathcal{N}_b(x) = \sum_{D \in \mathcal{D}_b(x)} \#\mathcal{N}_{b,D}(x) \leq x^{1-\beta/2}\#\mathcal{D}_b(x) < x^{1-\beta/2+\delta+o(1)} = o(x)$$

as $x \to \infty$, which is what we wanted to prove. □

4.1 Bell numbers

It is a straightforward calculation to check that condition (4.5) holds for all the sequences in Table 4.1, except for the Bell numbers which should be studied carefully. We denote by B_n the nth Bell number. In this case, the asymptotic estimate for B_n is given in terms of an implicit function $r = r(n)$ so the analysis of this concrete case should be made in detail. More concretely, we obtain the following corollary.

Corollary 12. *Let B_n denote the nth Bell number. For any base $b \geq 2$, the inequality*

$$s_b(B_n) > \frac{\log n}{60 \log b}$$

holds on a set of positive integers n of asymptotic density 1.

Proof. The study of Bell numbers needs of a more detailed analysis. We start with the following estimate for B_n (see formula (41) on page 562 in [43]).

Lemma 12. *Let $r := r(n)$, defined implicitly by*

$$re^r = n + 1. \tag{4.11}$$

Then

$$B_n = \frac{n! e^{e^r - 1}}{r^n \sqrt{2\pi r(r+1)e^r}} \left(1 + O\left(e^{-r/5}\right)\right). \tag{4.12}$$

The number $r := r(n)$ given in (4.11) satisfies $r = \log n - \log\log n + o(1)$ as $n \to \infty$, therefore

$$e^{-r/5} = \left(\frac{\log n}{n}\right)^{1/5}(1+o(1)) = O\left(n^{-1/6}\right) \quad \text{as} \quad n \to \infty. \tag{4.13}$$

Combining Stirling's formula (4.4) with formula (4.13) we can rewrite (4.12) as

$$B_n = e^{f(n)}\left(1 + O\left(n^{-1/6}\right)\right),$$

where

$$f(x) = x\log x - x - \left(\frac{2x+1}{2}\right)\log r + \frac{1}{2}\log x + e^r - \frac{r}{2} - \frac{1}{2}\log(r+1) - 1,$$

and $r := r(x)$ is defined for all real numbers $x \geq 1$ by equation (4.11) (where n is replaced by x). In particular, $r(x)$ has a derivative for real $x > 1$. In fact, differentiating the relation (4.11) (with x instead of n) with respect to the variable x, we have

$$r'e^r + rr'e^r = 1,$$

or equivalently

$$r'e^r = \frac{1}{r+1}, \tag{4.14}$$

and, since $e^r = (x+1)/r$,

$$r' = \frac{r}{(x+1)(r+1)}. \tag{4.15}$$

We get the asymptotic behavior of the second derivative of $f(x)$: observe that differentiating we have

$$\begin{aligned} f'(x) &= \frac{d}{dx}\left(x\log x - x - \frac{2x+1}{2}\log r + \frac{1}{2}\log x + e^r - \frac{r}{2} - \frac{1}{2}\log(r+1) - 1\right) \\ &= \log x - \log r - \frac{(2x+1)r'}{2r} + \frac{1}{2x} + r'e^r - \frac{r'}{2} - \frac{r'}{2(r+1)} \\ &= \log x - \log r + \frac{1}{2x} - e^{-r}\left(\frac{1}{2(r+1)^2} + \frac{1}{r+1} - \frac{1}{2r}\right), \end{aligned}$$

since, using equations (4.14) and (4.15), we note that

$$\begin{aligned} r'e^r - r'\left(\frac{(2x+1)(r+1) + r(r+1) + r}{2r(r+1)}\right) &= \frac{1}{r+1} - \frac{(2x+1)(r+1) + r(r+2)}{2(r+1)^2(x+1)} \\ &= -\frac{r^2 + r - 1}{2(x+1)(r+1)^2} \\ &= -e^{-r}\left(\frac{1}{2(r+1)^2} + \frac{1}{r+1} - \frac{1}{2r}\right). \end{aligned}$$

Differentiating the previous expression we obtain

$$\begin{aligned} &\frac{d}{dx}\left[-e^{-r}\left(\frac{1}{2(r+1)^2} + \frac{1}{r+1} - \frac{1}{2r}\right)\right] = \\ &\quad = r'e^{-r}\left(\frac{1}{(r+1)^3} + \frac{3}{2(r+1)^2} + \frac{1}{r+1} - \frac{1}{2r^2} - \frac{1}{2r}\right) \\ &\quad = \frac{r^2}{(x+1)^3}\left(\frac{1}{2(r+1)^3} + \frac{3}{2(r+1)^2} + \frac{1}{r+1} - \frac{1}{2r^2} - \frac{1}{2r}\right) = O(x^{-2}), \end{aligned}$$

therefore we can conclude that

$$f''(x) = \frac{1}{x} + \frac{r'}{r} + O(x^{-2}) = \frac{1}{x} + \frac{1}{(x+1)(r+1)} + O(x^{-2}) \asymp \frac{1}{x},$$

and we are under the assumptions of Theorem 18, and Corollary 12 holds. □

Chapter 5

Additive bases for intervals

Let G be a commutative semigroup. For two given subsets $A, B \subset G$ we define the function

$$r_{A+B}(x) = |\{(a,b) \in A \times B : \ a+b=x\}|.$$

In the case $A = B$ we denote by $r_A(x) = r_{A+A}(x)$ the representation function of A. Analogously, we define $d_A(x) = r_{A-A}(x)$.

There are many problems related to different restrictions on the representation function of a set or a sequence A, that have different solutions depending on the ambient conditions. As we discussed on Chapter 1 the simple restriction $r_A(x) \leq 2$, that is Sidon sets, directly implies that the set, if dense, is uniformly distributed in G when G is a finite group. Both Sidon sets and additive bases (sets with $r_A(x) \geq 1$) are very interesting objects and have been intensively studied in many different contexts.

In this chapter we will discuss some problems related to generalizations to these two basic concepts. If g is a positive integer and G a commutative semigroup: we say that A is a *g-Sidon* set if

$$r_A(x) \leq g \text{ for all } x \in G$$

and we say that A is a *g-basis* if

$$r_A(x) \geq g \text{ for all } x \in G.$$

If $r_A(x) \geq g$ for every $x \in I \subset G$ we say that A is a *g-basis for I*.

Given two positive real numbers $1 \leq g_1 \leq g_2$, we say that A is a $B[g_1, g_2]$ set if it is both g_1-basis and g_2-Sidon, that is

$$g_1 \leq r_A(x) \leq g_2 \text{ for all } x \in G.$$

If such a set A exists we say that $[g_1, g_2]$ is admissible for G. Clearly one could restrict to the case where g_i are integers, but this definition is more convenient and simplifies the notation in the following sections.

Deciding which pairs $[g_1, g_2]$ are admissible can be a difficult problem depending on the group or semigroup G we consider.

For example, if $G = \mathbb{Z}$ (or $\mathbb{Z}^k$), it is easy to show that $[g_1, g_2]$ is admissible for all $g_1, g_2 \in \mathbb{N}$, such that $1 \leq g_1 < g_2$. The case $g_1 = g_2$ is not admissible since the parity of the representation function must vary: those elements with a representation $a + a$ must have an odd value and the rest an even one.

However if $G = \mathbb{N}$, the problem is different and much more difficult. In fact, this question is far for being solved nor understood in this case.

Conjecture 2 (Erdős-Turán)**.** *Given any positive integers $1 \leq g_1 < g_2$, it does not exist a sequence of positive integers A such that*

$$g_1 \leq r_A(x) \leq g_2$$

for every large enough x.

It is clear that $g_1 = g_2$ is not possible because of the parity argument mentioned above. Dirac [37] proved that $r_A(x)$ cannot take only two positive values. It was proved in [52] that neither $[1, 5]$ nor $[1, 7]$ are admissible [9]. Sándor proved in [90] that if $g_1 > g_2 - 2\sqrt{g_2} + 1$ then $[g_1, g_2]$ is not admissible and, recently, Konstantoulas [64] showed that $\limsup r_A(x) \geq 6$ under the weaker assumption that the set $\mathbb{N} \setminus (A + A)$ has lower density less than $1/10$.

In the opposite direction there is an important result of Erdős-Rényi [39] which was the beginning of the probabilistic method applied to prove the existence of sequences with certain additive properties.

Theorem 19 (Erdős-Rényi)**.** *There exist positive constants $0 < c_1 < c_2$ and an infinite sequence of positive integers A with*

$$c_1 \log x < r_A(x) < c_2 \log x$$

for every large enough x.

This theorem gave an affirmative answer to a question of Sidon about the existence of additive bases with $r_A(x) \ll x^\epsilon$. However, this result does not imply the Erdős-Turán conjecture. The presence of the logarithm function is typical in the probabilistic method. Roughly speaking, the probabilistic method works because the random variables (such as $r_A(x)$) are concentrated around their expected values. In order to exploit that, it is needed that the expected value is not too small. With the probabilistic method it is possible to prove that for any $\epsilon > 0$ there exists a constant $C > 0$ and a sequence of positive integers A such that

$$C \log x < r_A(x) < C(1 + \epsilon) \log x$$

for every large enough x. Erdős conjectured that an asymptotic estimate of the form $r_A(x) \sim C \log x$ is not possible. This is an open problem.

Nevertheless, when G is a cyclic group, the problem changes drastically and Erdős-Turán Conjecture is not longer true in this context. This result appears implicitly in a paper of Ruzsa [88] devoted to prove that the Erdős-Turán conjecture is not true in quadratic mean.

Nowadays it is known [19] that for every cyclic group $\mathbb{Z}_m$ there is an additive basis A such that $r_A(x) \leq 288$ for all $x \in \mathbb{Z}_m$. Before Ruzsa's work, it was only known the existence of a set $A \subset \mathbb{Z}_m$ with $c_1 \log m < r_A(x) < c_2 \log m$, an analogous to Erdős -Rényi result for cyclic groups. Again it is possible to take $c_2 = c_1(1+\epsilon)$ when c_1 and m are large enough.

In Section 5.1 we show that if g_1 and g_2 are close enough, then for sufficiently large G the pair is not admissible.

Theorem 21. *If $g_2 < g_1 + 2\sqrt{g_1} + 1$ then $[g_1, g_2]$ is not admissible for any finite group G if $|G|$ is large enough.*

However, the true intention of this section is to construct sets with representation function as close as possible to a constant value in cyclic groups. To do so, we first find a construction for the group $\mathbb{Z}_p \times \mathbb{Z}_p$ and then project it to certain cyclic group, refining the ideas from [26].

Corollary 14. *If $g_2 > g_1 + 120 g_1^{4/5}$ then $[g_1, g_2]$ is admissible for an infinite family of cyclic groups $\mathbb{Z}_{m_i}$ with $m_i/m_{i+1} \to 1$.*

Note that, in this case, it is of vital importance for our applications that the numbers g_1, g_2 do not depend on the size of the group. We would need such a special set to prove analogous results to those obtained for g-Sidon sequences in [26] in the case of g-additive bases.

In [26], Cilleruelo, Ruzsa and Vinuesa applied the constructions of dense g-Sidon sets in cyclic groups to study the largest cardinality of a g-Sidon set in an interval. More precisely, define

$$\beta_g(n) = \max\{|A| : \ A \subset \{1, \dots, n\}, \ A \text{ is } g\text{-Sidon}\}$$

and the quantities

$$\underline{\beta_g} = \liminf_{n\to\infty} \frac{\beta_g(n)}{\sqrt{gn}}, \qquad \overline{\beta_g} = \limsup_{n\to\infty} \frac{\beta_g(n)}{\sqrt{gn}}.$$

The main result in this article is that both limits coincide when $g \to \infty$:

$$\lim_{g\to\infty} \underline{\beta_g} = \lim_{g\to\infty} \overline{\beta_g} = \sigma,$$

where σ is an explicit constant (although its numerical value is difficult to calculate; see, for example, [76]). More concretely $\sigma = \sup_{g\in\mathcal{G}} \|g\|_1$, where $\mathcal{G}$ is the family of non-negative real functions g with $\operatorname{supp}(g) \subseteq [0,1]$ such that $(g*g)(x) = \int_0^1 g(t)g(x-t)dt \leq 1$ for every $x \in [0,2]$.

This chapter is devoted to obtain analogous results for additive bases for intervals. If we define

$$\gamma_g(n) = \min\{|A| : \ A \text{ is } g\text{-basis for } \{1, \dots, n\}\}$$

it is easy to prove that $\sqrt{2n} \leq \gamma_1(n) \leq \sqrt{4n}$ but it is unknown if $\lim_{n\to\infty} \frac{\gamma_1(n)}{\sqrt{n}}$ exists.

We also define the quantities

$$\underline{\gamma_g} = \liminf_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}}, \qquad \overline{\gamma_g} = \limsup_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}}.$$

The main result in this chapter is the following:

Theorem 20.

$$\lim_{g\to\infty}\underline{\gamma_g} = \lim_{g\to\infty}\overline{\gamma_g} = \gamma$$

with

$$\gamma = \inf_{f\in\mathcal{F}} \|f\|_1$$

where $\mathcal{F}$ is the family of non-negative, integrable and bounded real functions f with $supp(f) \subseteq [-\frac{1}{4}, \frac{1}{4}]$ such that $(f*f)(x) = \int f(t)f(x-t)dt \geq 1$ for every $x \in [-1/2, 1/2]$.

With such result in mind, it is natural to wonder about the value of the constant γ and the following bounds are easy to obtain.

Proposition 8. *Let g be a positive integer. Then,*

$$1 \leq \underline{\gamma_g} \leq \overline{\gamma_g} \leq \sqrt{2}(1+o(1)).$$

Proof. The lower bound follows from the following observation: if A is a g-basis for $[1,n]$

$$|A|^2 = \sum_x r_A(x) \geq \sum_x g = gn.$$

For the upper bound, let us consider the set

$$A = \left\{(1-g)m, \dots, -m, 0, m \dots, m\left\lfloor\sqrt{\frac{ng}{2}}\right\rfloor\right\} \cup \left\{1, 2, \dots, \left\lfloor\sqrt{\frac{ng}{2}}\right\rfloor\right\},$$

where $m = \left\lceil\sqrt{2n/g}\right\rceil$. Clearly, $|A| = 2\left\lfloor\sqrt{\frac{ng}{2}}\right\rfloor + g = \sqrt{2ng}(1+o(1))$.

Observe that, for any $x \in \{1, \dots, n\}$ and any integer $1 \leq i \leq g/2$ there exists a unique representation of the form

$$x = x_1 + mx_2, \qquad (i-1)m \leq x_1 \leq im \quad \text{and} \quad x_2 \in \left\{1-g, \dots, -1, 0, 1, \dots, \left\lfloor\sqrt{\frac{ng}{2}}\right\rfloor\right\},$$

which gives at least g representations for x, two for each i since every pair $\{x_1, x_2\}$ gives arise to two different representations. □

It makes sense to modify the definition of $\gamma_g(n)$ by imposing some extra conditions on the support of A. For example, the classical problem assumes that $A \subset [0, n-1]$.

$$\gamma[n] = \min\{|A| : \ A \subset [0, n-1], \ A \text{ is an additive basis for } \{1, \dots, n\}\}.$$

The current records are due to Güntürk and Nathanson [53], for the upper bound, and Mrose [80], for the lower bound,

$$\sqrt{2.088n} \leq \gamma[n] \leq \sqrt{3.5002n}.$$

It is unknown if $\lim_{n\to\infty} \frac{\gamma[n]}{\sqrt{n}}$ exists.

Note that for any $\alpha > 1/2$, fixed g and sufficiently large n, we can consider the quantity

$$\gamma_g(\alpha, n) = \min\{|A| : \ A \subseteq [-\alpha n/2, \alpha n/2] \cap \mathbb{Z}, \ A \text{ is } g\text{-basis for } [-n/2, n/2]\},$$

and its limit when $\alpha \to \infty$ will be

$$\tilde{\gamma}_g(n) = \min\{|A| : A \subseteq \mathbb{Z},\ A \text{ is } g\text{-basis for } [-n/2, n/2]\}.$$

Observe that $\tilde{\gamma}_g(n) \neq \gamma_g(n)$ but asymptotically they are comparable when correctly normalized, that is, for every fixed g, $\lim_{n\to\infty} \frac{\gamma_g(n)-\tilde{\gamma}_g(n)}{\sqrt{n}} = 0$.

We can prove the analogous of the Theorem 20 for $\gamma_g(\alpha, n)$. That is, for any given real number $\alpha > 1/2$, we can define

$$\underline{\gamma_g}(\alpha) = \liminf_{n\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}}, \quad \overline{\gamma_g}(\alpha) = \limsup_{n\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \quad \text{and} \quad \gamma(\alpha) = \inf_{f\in\mathcal{F}_\alpha} \|f\|_1$$

where $\mathcal{F}_\alpha$ is the family of integrable nonnegative real bounded functions f with $\mathrm{supp}(f) \subseteq [-\alpha/2, \alpha/2]$ such that $(f * f)(x) = \int f(t)f(x-t)dt \geq 1$ for every $x \in [-1/2, 1/2]$. In order to prove the Theorem 20, we prove:

Theorem 27. *For every real number $\alpha > 1/2$,*

$$\lim_{g\to\infty} \underline{\gamma_g}(\alpha) = \lim_{g\to\infty} \overline{\gamma_g}(\alpha) = \gamma(\alpha).$$

Note that $\gamma(\alpha)$ is a non increasing function of α and that $\gamma = \lim_{\alpha\to\infty} \gamma(\alpha)$. We will obtain the Theorem 20 taking the limit when $\alpha \to \infty$.

5.1 Constructions in finite groups

In first place, let us analyse the range of admissibility for pairs on finite groups.

Theorem 21. *If $g_2 < g_1 + 2\sqrt{g}_1 + 1$ then $[g_1, g_2]$ is not admissible for a finite group G if $|G|$ is large enough.*

Proof. Suppose that A is a $B[g_1, g_2]$ in G.

Let $q = |G|$ and $t = |A|^2/q$. Obviously $g_1 \leq t \leq g_2$. Using the well known formulas

$$\sum_x r_A(x) = \sum_x d_A(x) = |A|^2 \qquad \text{and} \qquad \sum_x r_A^2(x) = \sum_x d_A^2(x)$$

we have for any y

$$\begin{aligned} \sum_x (r_A(x) - y)^2 &= \sum_x (r_A(x) - t)^2 + q(y-t)^2 \\ &= \sum_x (d_A(x) - t)^2 + q(y-t)^2 \\ &\geq (\sqrt{qt} - t)^2 + q(y-t)^2, \end{aligned}$$

since $d(0) = |A|$.

Now we take $y = (g_2 + g_1)/2$ and observe that $|r_A(x) - y| \leq (g_2 - g_1)/2$ for all $x \in G$. Thus,

$$\begin{aligned} q\left(\frac{g_2-g_1}{2}\right)^2 &> qt + q\left(\frac{g_1+g_2}{2} - t\right)^2 - 2t^{3/2}\sqrt{q} \\ \Longrightarrow \left(\frac{g_2-g_1}{2}\right)^2 &> t + \left(\frac{g_1+g_2}{2} - t\right)^2 - \frac{2g_2^{3/2}}{\sqrt{q}}. \end{aligned}$$

Writing $t = \frac{g_1+g_2}{2} - s$ we have

$$\left(\frac{g_2-g_1}{2}\right)^2 > \frac{g_2-g_1}{2} + g_1 - s + s^2 - \frac{2g_2^{3/2}}{\sqrt{q}}$$
$$\implies \left(\frac{g_2-g_1}{2} - \frac{1}{2}\right)^2 > g_1 + \frac{1}{4} - s + s^2 - \frac{2g_2^{3/2}}{\sqrt{q}} \geq g_1 - \frac{2g_2^{3/2}}{\sqrt{q}}.$$

Let $\epsilon > 0$ be the number such that $g_2 = g_1 + 2\sqrt{g_1} + 1 - \epsilon$. Then

$$\left(\sqrt{g_1} - \frac{\epsilon}{2}\right)^2 > g_1 - \frac{2g_2^{3/2}}{\sqrt{q}},$$

which is not possible if q is large enough. □

Corollary 13. *If $A + A = G$ and $|G|$ is large enough then $\max_x r_A(x) \geq 6$.*

Proof. Put $q = |G|$ and $m = |A|$ and suppose for a contradiction that A is 5-Sidon, so $m \leq \sqrt{5q}$. Since $A + A = G$ there are not $x \in G$ with $r_A(x) = 0$. The number of $x \in G$ with $r_A(x) \in \{1, 3, 5\}$ is less than or equal to m, since these elements must have at least one diagonal representation representation $a+a$ with $a \in A$ (non diagonal representations are even due to the reflexivity of representation $a + a' = a' + a$). Then

$$\sum_x (d_A(x) - 3)^2 = \sum_x (r_A(x) - 3)^2 = q + O(m) = q + O(\sqrt{q}).$$

The contribution of the term $x = 0$ to the left hand sum is $(m-3)^2$, since $d_A(0) = m$. Let r_2 denote the number of elements of G with $r_A(x) = 2$, the number of elements of G with $r_A(x) = 4$ is $q - r_2 + O(m)$. Since $\sum_x r_A(x) = m^2$, we have

$$(m-3)^2 = m^2 + O(m) = 2r_2 + 4(q - r_2) + O(m) = 4q - 2r_2 + O(\sqrt{q}).$$

Finally,

$$\sum_{x \neq 0} (d_A(x) - 3)^2 = q - 4q + 2r_2 + O(\sqrt{q}) = 2r_2 - 3q + O(\sqrt{q}) < -q + O(\sqrt{q}).$$

This sum of squares is < 0 if q is large enough, a contradiction. □

The next two theorems follow closely the lines of theorems 3.1 and 4.1 in [26] (inspired by some ideas in [88]). The main difference is that now we are not only interested in an upper bound for the number of representations of the elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ but also in a lower bound. We analyze carefully the number of representations of $(0,0) \in \mathbb{Z}_p \times \mathbb{Z}_p$, correcting a slight mistake in the original proof of Theorem 3.1 in [26]: if the parabolas A_u and A_{-u} were in our set A (see notation at the beginning of the proof of the next theorem), they would give p representations of $(0,0)$ and this case must be avoided. We also introduce a random set R together with $-R$ (the set with the opposites of the elements in R) in order to have enough representations of $(0,0)$.

Theorem 22. *If $g_2 > g_1 + 30g_1^{3/4}$, then $[g_1, g_2]$ is admissible for $\mathbb{Z}_p \times \mathbb{Z}_p$ for every prime $p \geq p_0(g_1)$.*

Proof. For every positive integer k and sufficiently large p depending on k, we will give an explicit construction of a set A with $k^2 - 2k^{3/2} - 2k \leq r_A(\mathfrak{a}) \leq k^2 + 2k^{3/2} + 24$ for every $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$.

For each nonzero element $u \in \mathbb{Z}_p$, we consider the parabola

$$A_u = \left\{ \left(x, \tfrac{x^2}{u} \right) : x \in \mathbb{Z}_p \right\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_p.$$

Our set A will be the union $S \cup R \cup -R$, where $S = A_{t+1} \cup \cdots \cup A_{t+k}$ is the union of k parabolas, for a suitable t, and R is a random subset of $\mathbb{Z}_p \times \mathbb{Z}_p$ with $\lfloor k^2/2 \rfloor$ elements.

Given $\mathfrak{a} = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ and $u, v \in \mathbb{Z}_p \setminus \{0\}$, we define the representation function

$$r_{u,v}(\mathfrak{a}) = |\{(\mathfrak{u}, \mathfrak{v}) \in A_u \times A_v : \mathfrak{u} + \mathfrak{v} = \mathfrak{a}\}|,$$

or, equivalently, the number of solutions $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the system of equations

$$\begin{cases} x + y & \equiv a \pmod{p}, \\ \frac{x^2}{u} + \frac{y^2}{v} & \equiv b \pmod{p}. \end{cases} \tag{5.1}$$

We need good estimates for this function in order to select a proper set of parabolas. The next Lemma gives us an important property and was included in [26].

Lemma 13. *Let $u, v, u', v' \in \mathbb{Z}_p \setminus \{0\}$ such that $u + v \equiv u' + v'$ and $u \not\equiv -v$. If $\left(\frac{uvu'v'}{p}\right) = -1$, where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, then*

$$r_{u,v}(\mathfrak{a}) + r_{u',v'}(\mathfrak{a}) = 2$$

for every $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. For a fixed $\mathfrak{a} = (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$. If $a \equiv x + y$ and $b = \frac{x^2}{u} + \frac{y^2}{v}$, with $uv \not\equiv 0$, then $(u + v)x^2 - 2aux + u(a^2 - bv) \equiv 0$. Since $u \not\equiv -v$ the number of solutions of this equation is $r_{u,v}(\mathfrak{a}) = 1 + \left(\frac{\Delta}{p}\right)$, where $\Delta \equiv 4uv((u + v)b - a^2)$.

Then it is sufficient to show that $\left(\frac{\Delta}{p}\right) + \left(\frac{\Delta'}{p}\right) = 0$. This is obviously true if $(u+v)b - a^2 \equiv 0$, since $u + v \equiv u' + v'$. If not, $\Delta\Delta' \equiv 16uvu'v'((u + v)b - a^2)^2$ and

$$\left(\tfrac{\Delta}{p}\right)\left(\tfrac{\Delta'}{p}\right) = \left(\tfrac{uvu'v'}{p}\right)\left(\tfrac{((u+v)b-a^2)^2}{p}\right) = -\left(\tfrac{((u+v)b-a^2)^2}{p}\right) = -1,$$

which completes the proof of the Lemma. □

Now we write

$$S = \bigcup_{u=t+1}^{t+k} A_u,$$

and we will find a suitable t such that S will be good for our purposes. It is clear that $|S| = k(p - 1) + 1$, since every parabola contains exactly p points and the origin is the only element they share.

We observe that in the case $u \equiv -v$ we deal with the linear equation $2aux - u(a^2 - bv) \equiv 0$, which would give p solutions to (5.1), if $(a, b) = (0, 0)$. Therefore we must exclude this possibility in our set S to avoid many representations of $(0, 0)$. We will impose $t \notin [(p+1)/2 - k, (p-3)/2]$ to avoid it.

Finally, we look at the number of representations $r_S(\mathfrak{a})$ for all nonzero elements $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$. We can estimate the representation function of S as

$$\sum_{u,v=t+1}^{t+k} r_{u,v}(\mathfrak{a}) - 2k \leq r_S(\mathfrak{a}) \leq \sum_{u,v=t+1}^{t+k} r_{u,v}(\mathfrak{a}), \tag{5.2}$$

depending on whether or not $\mathfrak{a} \in A_u$ for some u, for every $\mathfrak{a} \neq (0, 0)$. Note that if $\mathfrak{a} \in A_u$ for some u, provided that the element $(0, 0)$ lies on every parabola, we would be overcounting $2k$ representations in this case.

Let us parametrize the variables on the sum as follows: $u = t+i$, $v = t+j$ with $1 \leq i, j \leq k$. Clearly, for every pair u, v we have $i + j = k + 1 + l$ for some $|l| \leq k - 1$.

For a fixed l, there are exactly $k - |l|$ pairs (i, j) (resp. (u, v)). Those pairs can be divided into two sets depending on the quadratic residue of uv modulo p. Say that n^+ of them have $\left(\frac{uv}{p}\right) = 1$ and n^- of them have $\left(\frac{uv}{p}\right) = -1$. Clearly $n^+ + n^- = k - |l|$, and

$$n^+ - n^- = \sum \left(\tfrac{uv}{p}\right).$$

This means that one can combine $\min\{n^+, n^-\}$ pairs (u, v, u', v') with $\left(\frac{uvu'v'}{p}\right) = -1$.

Therefore, by means of Lemma 13, we have that

$$2\min\{n^+, n^-\} \leq \sum_{i+j=k+1+l} r_{u,v}(\mathfrak{a}) \leq 2\max\{n^+, n^-\}$$

since for every pair (u, v) and every $\mathfrak{a} \neq (0, 0)$ we trivially have $0 \leq r_{u,v}(\mathfrak{a}) \leq 2$, and $2\min\{n^+, n^-\} + 2\left(\max\{n^+, n^-\} - \min\{n^+, n^-\}\right) = 2\max\{n^+, n^-\}$.

Or, equivalently,

$$k - |l| - \left|\sum \left(\tfrac{uv}{p}\right)\right| \leq \sum_{i+j=k+1+l} r_{u,v}(\mathfrak{a}) \leq k - |l| + \left|\sum \left(\tfrac{uv}{p}\right)\right|. \tag{5.3}$$

Summing up over all possible values of l in (5.3) and taking into account the bounds in (5.2) we have, for every fixed t,

$$k^2 - \mathcal{S}(t) - 2k \leq r_S(\mathfrak{a}) \leq k^2 + \mathcal{S}(t), \tag{5.4}$$

where

$$\mathcal{S}(t) = \sum_{|l| \leq k-1} \left| \sum_{i+j=k+1+l} \left(\tfrac{(t+i)(t+j)}{p}\right) \right|.$$

We will now show that there exists at least one $t \notin [p-k, p-1] \cup [(p-1)/2 - k, (p-3)/2]$, for which $\mathcal{S}(t)$ is small. Recall that $t \notin [p-k, p-1]$ prevents us from choosing $u \equiv 0$ and $t \notin [(p-1)/2 - k, (p-3)/2]$ avoids the case $u + v \equiv 0$.

We will first show that this quantity is small on average. Applying the Cauchy-Schwarz inequality we obtain

$$\begin{aligned}\sum_{t=0}^{p-1}\mathcal{S}(t) &= \sum_{t,l}\left|\sum_{i+j=k+1+l}\left(\tfrac{(t+i)(t+j)}{p}\right)\right| \\ &\le \sqrt{2kp\sum_{t,l}\left(\sum_{i+j=k+1+l}\left(\tfrac{(t+i)(t+j)}{p}\right)\right)^2} \\ &= \sqrt{2kp\sum_{i+j=i'+j'}\sum_{t}\left(\tfrac{(t+i)(t+j)(t+i')(t+j')}{p}\right)}.\end{aligned}$$

Weil's Theorem assures that

$$\left|\sum_{t=0}^{p-1}\left(\tfrac{(t+i)(t+j)(t+i')(t+j')}{p}\right)\right| \le 4\sqrt{p},$$

whenever the numerator, as a polynomial of t, is a square. This case corresponds to the case when i,j,i',j' form two equal pairs, which happens exactly $k(2k-1)$ times. In this case the sum is either p or $-p$.

Combining these estimates we have

$$\sum_{t=0}^{p-1}\mathcal{S}(t) \le \sqrt{2p^2k^2(2k-1)+8p^{3/2}k^4},$$

since there are less than k^3 possible quadruples i,j,i',j'. In particular, this implies that there exists a value of $t \notin [p-k,p-1]\cup[(p-1)/2-k,(p-3)/2]$ such that

$$\mathcal{S}(t) \le \frac{\sqrt{2p^2k^2(2k-1)+8p^{3/2}k^4}}{p-2k} < 2k^{3/2} \tag{5.5}$$

for sufficiently large p.

Since we excluded the possibility $u \equiv -v$, then $(0,0)+(0,0)$ is the only representation of $(0,0)$ as a sum of two elements of S; i.e. $r_S((0,0))=1$. That is why we include a set R chosen at random from all the subsets of $\mathbb{Z}_p\times\mathbb{Z}_p$ with $\lfloor k^2/2\rfloor$ elements and the set with the opposites or its elements, $-R$, to obtain at least $2\lfloor k^2/2\rfloor-1$ (and at most $2\lfloor k^2/2\rfloor$) representations of $(0,0)$ as a sum of two elements of $R\cup -R$ (observe that one of them could be $(0,0)+(0,0)$ since R is random and can share elements with S). Then

$$2\lfloor k^2/2\rfloor - 1 \le r_S((0,0)) + r_{R-R}((0,0)) + r_{-R+R}((0,0)) \le 2\lfloor k^2/2\rfloor + 1. \tag{5.6}$$

Now, we have to check that, for an appropriate choice of R, the addition of R and $-R$ does not add many representations of any nonzero element.

First we study $r_{S+R}(\mathfrak{a})$ for every $\mathfrak{a}$. The probability that a random element of $\mathbb{Z}_p\times\mathbb{Z}_p$ is in S (or in any set with the same number of elements) is the quotient $\frac{|S|}{|\mathbb{Z}_p\times\mathbb{Z}_p|} = \frac{kp-k+1}{p^2}$, so the

probability that, for a fixed $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$, one element of R is in $\mathfrak{a} - S$ is exactly that. Then, the probability that, for a fixed $\mathfrak{a}$, there are three elements of R in $\mathfrak{a} - S$ is

$$\leq \binom{\lfloor k^2/2 \rfloor}{3} \left(\frac{kp-k+1}{p^2}\right)^3 \leq \binom{k^2/2}{3} \left(\frac{k}{p}\right)^3 \leq \frac{k^9}{p^3}.$$

This means that the probability that $r_{S+R}(\mathfrak{a})$ is greater than or equal to 3 for some $\mathfrak{a}$ is $\leq \frac{k^9}{p}$. The same applies to $r_{S-R}(\mathfrak{a})$ so, if $p > k^9/0.1$, we have

$$\mathbb{P}\left((r_{S+R}(\mathfrak{a}) \geq 3 \cup r_{S-R}(\mathfrak{a}) \geq 3) \text{ for some } \mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p\right) \leq 0.1 + 0.1 = 0.2.$$

Now we study $r_{R+R}(\mathfrak{a})$. Given any $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$, we can make p^2 pairs of elements of $\mathbb{Z}_p \times \mathbb{Z}_p$ adding up to $\mathfrak{a}$ that we can split into one pair $(\mathfrak{a}/2, \mathfrak{a}/2)$ and $\frac{p^2-1}{2}$ couples of pairs $(\mathfrak{n}, \mathfrak{a}-\mathfrak{n})$, $(\mathfrak{a}-\mathfrak{n}, \mathfrak{n})$. For a fixed $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$, the probability that $r_{R+R}(\mathfrak{a}) \geq 4$ is

$$\leq \frac{\binom{\frac{p^2-1}{2}}{\binom{p^2-4}{\lfloor \frac{k^2}{2} \rfloor - 4}}}{\binom{p^2}{\lfloor \frac{k^2}{2} \rfloor}} = \frac{\lfloor \frac{k^2}{2} \rfloor \left(\lfloor \frac{k^2}{2} \rfloor - 1\right)\left(\lfloor \frac{k^2}{2} \rfloor - 2\right)\left(\lfloor \frac{k^2}{2} \rfloor - 3\right)}{8p^2(p^2-2)} \leq \frac{k^8}{p^2(p^2-2)}.$$

Then the probability that $r_{R+R}(\mathfrak{a})$ is greater than or equal to 4 for some $\mathfrak{a}$ is $\leq \frac{k^8}{p^2-2}$. The same applies to $r_{-R-R}(\mathfrak{a})$ so, if $p > \sqrt{k^8 + 0.2}$, we have

$$\mathbb{P}\left((r_{R+R}(\mathfrak{a}) \geq 4 \cup r_{-R-R}(\mathfrak{a}) \geq 4) \text{ for some } \mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p\right) \leq 0.1 + 0.1 = 0.2.$$

Finally we study $r_{R-R}(\mathfrak{a})$. Given any $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$, we can make p^2 pairs with difference $\mathfrak{a}$. For any $\mathfrak{a} \neq (0,0)$, the two elements each one of the p^2 pairs, $(\mathfrak{n}, \mathfrak{n}-\mathfrak{a})$, are different (and every element of $\mathbb{Z}_p \times \mathbb{Z}_p$ appears in exactly two of the pairs). Now, for a fixed nonzero $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$ and for $p \neq 3$ it cannot happen that $\mathfrak{e} - \mathfrak{f} = \mathfrak{a}$, $\mathfrak{g} - \mathfrak{e} = \mathfrak{a}$ and $\mathfrak{f} - \mathfrak{g} = \mathfrak{a}$ at the same time, and so the probability that $r_{R-R}(\mathfrak{a}) \geq 2$ is

$$\leq \frac{p^2(p^2-3)\binom{p^2-4}{\lfloor \frac{k^2}{2} \rfloor - 4} + 2p^2\binom{p^2-3}{\lfloor \frac{k^2}{2} \rfloor - 3}}{\binom{p^2}{\lfloor \frac{k^2}{2} \rfloor}} \leq \frac{k^6(k^2+1)}{(p^2-1)(p^2-2)}.$$

Then the probability that $r_{R-R}(\mathfrak{a})$ is greater than or equal to 2 for some nonzero $\mathfrak{a}$ is $\leq \frac{p^2k^6(k^2+1)}{(p^2-1)(p^2-2)}$ and, again, for sufficiently large p depending on k, we have

$$\mathbb{P}\left(r_{R-R}(\mathfrak{a}) \geq 2 \text{ for some nonzero } \mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p\right) \leq 0.1.$$

Since, for every $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$, $r_{S+R}(\mathfrak{a}) = r_{R+S}(\mathfrak{a})$ and $r_{R-R}(\mathfrak{a}) = r_{-R+R}(\mathfrak{a})$ then

$$\mathbb{P}\left(r_{S\cup R\cup -R}(\mathfrak{a}) - r_S(\mathfrak{a}) \geq 24 \text{ for some nonzero } \mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p\right) \leq 0.2 + 0.2 + 0.1 = 0.5,$$

where the number 24 comes from 6 (from $S+R$ and $R+S$) plus 6 (from $S-R$ and $-R+S$) plus 4 (from $R+R$) plus 4 (from $-R-R$) plus 4 (from $R-R$ and $-R+R$). Since this has positive probability it means that there is a choice of R for which it is satisfied.

Combining this with (5.4) and (5.5) we can deduce that there exists choices of t and R such that, if $A = S \cup R \cup -R$,

$$k^2 - 2k^{3/2} - 2k \leq r_A(\mathfrak{a}) \leq k^2 + 2k^{3/2} + 24 \tag{5.7}$$

for every $\mathfrak{a} \in \mathbb{Z}_p \times \mathbb{Z}_p$ (including $(0,0)$ because of (5.6)).

Given g_1, we choose k such that $(k-1)^2 - 2(k-1)^{3/2} - 2(k-1) \leq g_1 \leq k^2 - 2k^{3/2} - 2k$. Observe that since $g_1 \geq 1$, then $k \geq 9$ and

$$g_1 \geq k^2 - 2(k-1)^{3/2} - 2k + 3 \geq k^2 - 4k^{3/2},$$

since $4k \leq 2k^{3/2}$. It is also true that,

$$g^{3/4} \geq \left(k^2 - 4k^{3/2}\right)^{3/4} = k^{3/2}\left(1 - \frac{4}{k^{1/2}}\right)^{3/4} \geq k^{3/2}2^{-3/4}.$$

Since we now know how to construct a $B[k^2 - 2k^{3/2} - 2k, k^2 + 2k^{3/2} + 24]$ set in $\mathbb{Z}_p \times \mathbb{Z}_p$ (see (5.7)) it will be enough if $g_2 \geq k^2 + 2k^{3/2} + 24$. Observe that it follows from the previous estimates for g_1 that

$$g_2 > g_1 + 30g_1^{3/4} \geq k^2 + (30 \cdot 2^{-3/4} - 4)k^{3/2} \geq k^2 + 3k^{3/2} \geq k^2 + 2k^{3/2} + 24.$$

This proves that $[g_1, g_2]$ is admissible in the proposed range. □

5.1.1 Good constructions in cyclic groups

Theorem 23. *If $[g_1, g_2]$ is admissible for $\mathbb{Z}_p \times \mathbb{Z}_p$ then $[g_1(s-1), g_2(s+1)]$ is admissible for $\mathbb{Z}_{p^2 s}$ for every positive integer s.*

Proof. Let $A \subset \mathbb{Z}_p \times \mathbb{Z}_p$ be a $B[g_1, g_2]$ set with m elements. We will construct a set $A' \subseteq \mathbb{Z}_{p^2 s}$ with ms elements satisfying

$$g_1(s-1) \leq r_{A'}(t) \leq g_2(s+1),$$

for every $t \in \mathbb{Z}_{p^2 s}$.

For a given element $(a,b) \in A$, we represent it by the corresponding residues in $[0, p-1]$. The set A' contains all the elements of the form

$$a + cp + bps$$

with $c \in [0, s-1]$ and $a, b \in [0, p-1]$ where $(a,b) \in A$.

Since $a + cp + bps$ is different for each three possible values of $a \in [0, p-1]$, $b \in [0, p-1]$ and $c \in [0, s-1]$, and since $0 \leq a + cp + bps \leq p - 1 + (s-1)p + (p-1)ps = p^2 s - 1$, it is clear that $|A'| = ms$. It is also clear that every element of $\mathbb{Z}_{p^2 s}$ can be written (in a unique way) as $x + yp + zps$ for some $x, z \in [0, p-1]$ and $y \in [0, s-1]$.

Given $x + yp + zps \in \mathbb{Z}_{p^2 s}$ we want to bound $r_{A'}(x + ys + zps)$, its number of representations as sum of two elements of A':

$$x + yp + zps \equiv a_1 + c_1 p + b_1 ps + a_2 + c_2 p + b_2 ps \pmod{p^2 s}. \tag{5.8}$$

In other words, we want to count the number of pairs $(a_1, c_1, b_1), (a_2, c_2, b_2)$ satisfying equation (5.8) such that (a_1, b_1) and (a_2, b_2) are in A and $c_1, c_2 \in [0, s-1]$.

We consider equation (5.8) modulo p:

$$x \equiv a_1 + a_2 \pmod{p},$$

and, since $0 \leq a_1 + a_2 \leq 2p - 2$, this implies that $x + \alpha p = a_1 + a_2$, where α is either 0 or 1. Informally, α says 'if we carry one or not when adding up a_1 and a_2'.

We substitute this into (5.8) and substract $a_1 + a_2$ from both sides:

$$yp + zps \equiv \alpha p + c_1 p + b_1 ps + c_2 p + b_2 ps \pmod{p^2 s},$$

or, equivalently,

$$y + zs \equiv \alpha + c_1 + c_2 + (b_1 + b_2)s \pmod{ps}. \tag{5.9}$$

Again, considering equation (5.9) modulo s, we have:

$$y \equiv \alpha + c_1 + c_2 \pmod{s},$$

and, since $0 \leq \alpha + c_1 + c_2 \leq 2s - 1$, this implies that $y + \beta s = \alpha + c_1 + c_2$, where β is either 0 or 1. Informally, β says 'if we carry one or not when adding up c_1, c_2 and α'.

We substitute this into (5.9) and substract $\alpha + c_1 + c_2$ from both sides:

$$zs \equiv \beta s + b_1 s + b_2 s \pmod{ps},$$

or, equivalently,

$$z \equiv \beta + b_1 + b_2 \pmod{p}.$$

Given x, y and z, we look for representations in $\mathbb{Z}_p \times \mathbb{Z}_p$ of

$$(x, z) = (a_1, b_1) + (a_2, b_2) \tag{5.10}$$

and

$$(x, z - 1) = (a_1, b_1) + (a_2, b_2) \tag{5.11}$$

with (a_1, b_1) and (a_2, b_2) in A. Equation (5.10) corresponds to the representations with $\beta = 0$ and equation (5.11) corresponds to the representations with $\beta = 1$.

If we call the number of solutions of (5.10) and (5.11) $r_A((x, z))$ and $r_A((x, z - 1))$ respectively, we know that

$$g_1 \leq r_A((x, z)) \leq g_2 \qquad \text{and} \qquad g_1 \leq r_A((x, z - 1)) \leq g_2.$$

Now we have to look at the possible values of c_1 and c_2 for each one of these solutions.

If we have (a_1, b_1) and (a_2, b_2) coming from (5.10) then we want

$$c_1 + c_2 = y - \alpha.$$

There are $y - \alpha + 1$ representations of this number with c_1 and c_2 in $[0, s - 1]$: $c_1 = 0$ and $c_2 = y - \alpha$, $c_1 = 1$ and $c_2 = y - \alpha - 1$, ..., $c_1 = y - \alpha$ and $c_2 = 0$.

The value of α depends on a_1 and a_2 but is either 0 or 1, so the number of representations of $x+yp+zps$ as a sum of two elements of A' with (a_1,b_1) and (a_2,b_2) coming from (5.10) is between yg_1 and $(y+1)g_2$.

If we have (a_1,b_1) and (a_2,b_2) coming from (5.11) then we want

$$c_1+c_2=y+s-\alpha.$$

There are $s+\alpha-1-y$ representations of this number with c_1 and c_2 in $[0,s-1]$: $c_1=y+1-\alpha$ and $c_2=s-1$, $c_1=y+2-\alpha$ and $c_2=s-2$, ..., $c_1=y+(s+\alpha-1-y)-\alpha=s-1$ and $c_2=s-(s+\alpha-1-y)=y+1-\alpha$.

Thus, the number of representations of $x+yp+zps$ as a sum of two elements of A' with (a_1,b_1) and (a_2,b_2) coming from (5.11) is between $(s-1-y)g_1$ and $(s-y)g_2$.

Observe that the number of representations $r_{A'}(x+yp+zps)$ is obtained after combining those arising from equations (5.10) and (5.11), that we have already estimated. Adding these results, we have that for given x, y and z, the number of representations of $x+yp+zps$ as a sum of two elements of A' is

$$(s-1)g_1\le r_{A'}(x+yp+zps)\le(s+1)g_2.$$

□

Putting together our work, we easily obtain then following corollary.

Corollary 14. *If $g_2>g_1+120g_1^{4/5}$ then $[g_1,g_2]$ is admissible for an infinite family of cyclic groups $\mathbb{Z}_{m_i}$ with $m_i/m_{i+1}\to 1$.*

Proof. Given $1\le g_1\le g_2$ we write $g_1=h_1(s-1)$ and $g_2=h_2(s+1)$. Observe that by Theorem 22 it suffices to show that if $g_2-g_1\ge 120g_1^{4/5}$, then $h_2-h_1\ge 30h_1^{3/4}$ for some integer s.

Choose $s=\lceil g_1^{1/5}\rceil+1$, which implies that $g_1^{4/5}/2\le h_1\le g_1^{4/5}$. Then,

$$h_2-h_1>\frac{g_2-g_1+2h_1}{s+1}\ge\frac{g_2-g_1+g^{4/5}}{4g^{1/5}}\ge\frac{121}{4}g^{3/5}\ge 30h_1^{3/4}.$$

It follows from Theorem 22 that, for every sufficiently large prime p, $[h_1,h_2]$ is admissible for $\mathbb{Z}_p\times\mathbb{Z}_p$. We now deduce from Theorem 23 that $[h_1(s-1),h_2(s+1)]=[g_1,g_2]$ is admissible for the cyclic group $\mathbb{Z}_{p^2s}$ for every sufficiently large prime p. □

We write another corollary, based on the proofs of Theorems 22 and 23, in a more convenient way for our purposes in Section 5.3.1.

Corollary 15. *For every positive integers k and s and for every prime $p\ge p_0(k)$, there is a set $A\subseteq\mathbb{Z}_{p^2s}$ with $|A|=\left(kp-k+1+2\lfloor\frac{k^2}{2}\rfloor\right)s$ and*

$$r_{A+A}(a)\in[(k^2-2k^{3/2}-2k)(s-1),(k^2+2k^{3/2}+24)(s+1)]$$

for every $a\in\mathbb{Z}_{p^2s}$.

5.2 Obtaining a function from a set

Theorem 24. *For every real number $\alpha > 1/2$ and for every positive integer g,*

$$\liminf_{n\to\infty} \frac{\gamma_g(\alpha, n)}{\sqrt{gn}} \geq \gamma(\alpha).$$

Proof. For every $\epsilon > 0$, for fixed $\alpha > 1/2$ and given integers g and $n \geq n_0 = \max\{\frac{4(\alpha+g)}{2\alpha-1}, 16g\epsilon^{-2}\}$, let $A \subseteq [-\alpha(n-2)/2, \alpha(n-2)/2]$ be a g-basis for $[-n/2+1, n/2-1]$. By adding at most $4g$ elements to it we can easily obtain a g-basis for $[-n/2-1, n/2+1]$, namely A', also supported in $[-\alpha(n-2)/2, \alpha(n-2)/2]$ (here we have used the condition $n \geq \frac{4(\alpha+g)}{2\alpha-1}$ since this implies $\lfloor \frac{\alpha(n-2)}{2} \rfloor - (g-1) \geq (\frac{n}{2}+1)/2)$.

Let us define the following step function f

$$f(x) = \sqrt{\frac{n}{g}} \text{ if } x \in \left[\frac{i}{n} - \frac{1}{2n}, \frac{i}{n} + \frac{1}{2n}\right] \text{ and } i \in A'$$

and $f(x) = 0$ in other case. Observe that

$$supp(f) \subseteq \left[-\frac{\alpha}{2}, \frac{\alpha}{2}\right].$$

The convolution $f * f$ is a continuous piecewise linear function which, in particular, interpolates linearly the values

$$(f * f)\left(\frac{i}{n}\right) = \frac{r_{A'}(i)}{g} \text{ for integers } i \in [-n/2-1, n/2+1],$$

and so

$$f * f(x) \geq 1 \text{ for every } x \in [-1/2, 1/2].$$

So $f \in \mathcal{F}_\alpha$ (see definition at the end of the previous section) and, since $n \geq 16g\epsilon^{-2}$,

$$\int f(x)dx = \frac{|A'|}{\sqrt{gn}} \leq \frac{|A| + 4g}{\sqrt{gn}} \leq \frac{|A|}{\sqrt{gn}} + \epsilon,$$

which completes the proof. □

If $\alpha \geq 1$ then $\frac{4(\alpha+g)}{2\alpha-1} \leq 4(g+1)$ and then n_0 depends only on g and ϵ and not on α.

In particular:

Corollary 16. *For every real number $\alpha > 1/2$,*

$$\liminf_{g\to\infty} \liminf_{n\to\infty} \frac{\gamma_g(\alpha, n)}{\sqrt{gn}} \geq \gamma(\alpha).$$

5.3 Obtaining a set from a function

In this section we use the Probabilistic Method to obtain a set whose representation function approximates the autoconvolution of a given function. There exist previous results in this line (see, for example [40]). Here we obtain a more appropriate result for our purposes.

Theorem 25. *Let $\delta = \delta(n)$ be a positive function of n satisfying $\delta(n) \to 0$ and $n\delta(n)/\log n \to \infty$ when $n \to \infty$. Let f be a positive, integrable and bounded function supported on a symmetric interval $I = [-a, a]$. For any $\epsilon > 0$ and $n > n(\epsilon, f)$ there exists a set of integers $A \subseteq [-an, an]$ such that*

$$\left| \frac{r_A(m)}{n\delta} - (f * f)(m/n) \right| \leq \epsilon \quad \text{for every integer } \ m \in [-2an + \delta n/2, 2an - \delta n/2]$$

and

$$\left| \frac{|A|}{n\delta^{1/2}} - \int f(x)dx \right| \leq \epsilon \int f(x)dx.$$

Proof. We follow here, as done in [26], the idea of Schinzel and Schmidt in [91] of taking the integral of f in overlapping intervals to obtain a discrete version of it and then we use these values as probabilities to construct a random set A.

For each integer $i \in [-an, an]$ define $I_i = \left\{x \in \mathbb{R} : \left|\frac{i}{n} - x\right| \leq \frac{\delta}{2}\right\}$ and let $I_i(x)$ be the characteristic function of I_i. Define I_i with $i \notin [-an, an] \cap \mathbb{Z}$ (either because $i < -an$, $i > an$ or $i \notin \mathbb{Z}$) as $I_i = \emptyset$ and $I_i(x) \equiv 0$. We observe that, at least for sufficiently large n, the intervals I_i overlap (since $\delta \gg \log n/n$ by assumption) and some of them are not included in $[-a, a]$.

Let us consider the probabilistic space where the events $i \in A$ are independent and $\mathbb{P}(i \in A) = \delta^{-1/2} \int_{I_i} f(x)dx$. Observe that, for sufficiently large n, this quantity is less than 1 for every i.

For every integer $m \in [-2an, 2an]$, denote $r_{A\hat{+}A}(m) = |\{(b, b') : \ b, b' \in A, \ b \neq b', \ b + b' = m\}|$. We have removed the possible representation $b + b = m$ for technical reasons (it is convenient for the calculations that the events $b \in A$ and $m - b \in A$ are independent).

We can write

$$r_{A\hat{+}A}(m) = X(m) = \sum_{i \neq m/2} X_i(m),$$

where, for every integer $i \in [an, an]$, $X_i(m)$ is defined as the boolean random variable

$$X_i(m) = \begin{cases} 1 & \text{if } i, m - i \in A, \\ 0 & \text{otherwise.} \end{cases}$$

We have that for $i \neq m/2$

$$\begin{aligned} \mathbb{E}(X_i(m)) &= \mathbb{P}(i \in A)\mathbb{P}(m - i \in A) \\ &= \frac{1}{\delta} \int_{I_i} f(x)dx \int_{I_{m-i}} f(y)dy \\ &= \frac{1}{\delta} \iint f(x)f(y)I_i(x)I_{m-i}(y)dxdy. \end{aligned}$$

Observe that this includes, for example, the case when i or $m-i$ are not in $[-an, an] \cap \mathbb{Z}$; in that case one of the indicator functions I_i or I_{m-i} is 0 and so are $X_i(m)$ and its expectation.

With this observation in mind, we have

$$\begin{aligned}
\mathbb{E}(X(m)) &= \sum_{i \neq m/2} \mathbb{E}(X_i(m)) \\
&= 2\delta^{-1} \sum_{i<m/2} \int_{I_i} f(x)dx \int_{I_{m-i}} f(y)dy \\
&= \frac{1}{\delta} \iint f(x)f(y) \sum_{i \neq m/2} I_i(x)I_{m-i}(y)dxdy \\
&= \frac{1}{\delta} \iint f(x)f\left(\tfrac{m}{n} - x + z\right) \sum_{i \neq m/2} I_i(x)I_{m-i}\left(\tfrac{m}{n} - x + z\right) dxdz \\
&= \frac{1}{\delta} \iint f(x)f\left(\tfrac{m}{n} - x\right) \sum_{i \neq m/2} I_i(x)I_{m-i}\left(\tfrac{m}{n} - x + z\right) dxdz \\
&+ \frac{1}{\delta} \iint f(x)\left(f\left(\tfrac{m}{n} - x + z\right) - f\left(\tfrac{m}{n} - x\right)\right) \sum_{i \neq m/2} I_i(x)I_{m-i}\left(\tfrac{m}{n} - x + z\right) dxdz.
\end{aligned}$$

Recall that, as long as $m - i \in [-an, an]$, we have $I_i(x)I_{m-i}(\frac{m}{n} - x + z) = I_i(x)I_i(x - z)$, since

$$\left|\tfrac{m-i}{n} - \left(\tfrac{m}{n} - x + z\right)\right| = \left|\tfrac{i}{n} - (x - z)\right|.$$

If not, it follows that $I_{m-i} \equiv 0$ while I_i may not. Therefore

$$\begin{aligned}
\mathbb{E}(X(m)) &= \frac{1}{\delta} \iint f(x)f\left(\tfrac{m}{n} - x + z\right) \sum_{i=m-n/2}^{m+n/2} I_i(x)I_i\left(x - z\right) dxdz + O(1) \\
&= \frac{1}{\delta} \iint f(x)f\left(\tfrac{m}{n} - x\right) \sum_{i=m-an}^{m+an} I_i(x)I_i\left(x - z\right) dxdz + O(1) \\
&\quad + \frac{1}{\delta} \iint f(x)\left(f\left(\tfrac{m}{n} - x + z\right) - f\left(\tfrac{m}{n} - x\right)\right) \sum_{i=m-an}^{m+an} I_i(x)I_i\left(x - z\right) dxdz \\
&\quad \delta^{-1} \iint f(x)f\left(\frac{m}{n} - x\right) \sum_{i=\max\{1,m-n\}}^{\min\{m-1,n\}} I_i(x)I_i\left(x - z\right) dxdz \\
&\quad + \delta^{-1} \iint f(x)\left(f\left(\frac{m}{n} - x + z\right) - f\left(\frac{m}{n} - x\right)\right) \cdot \\
&\quad \sum_{i=\max\{1,m-n\}}^{\min\{m-1,n\}} I_i(x)I_i\left(x - z\right) dxdz + O(1) \\
&= J_1 + J_2 + O(1),
\end{aligned}$$

where the $O(1)$ term comes from the term with $i = m/2$ that we have added to the sum and the fact that $f * f$ is bounded.

It is convenient to define $S(x,z)=\sum_i I_i(x)I_i(x-z)$. Let us recall that the sum is taken over all integers

$$i\in[-an,an]\cap[-an+m,an+m] \tag{5.12}$$

and counts the number of integers i for which $x,x-z\in I_i$ or, equivalently, the number of integers

$$i\in\left[nx-\tfrac{\delta n}{2},nx+\tfrac{\delta n}{2}\right]\cap\left[n(x-z)-\tfrac{\delta n}{2},n(x-z)+\tfrac{\delta n}{2}\right]. \tag{5.13}$$

It is clear that for $|z|>\delta$ we have $S(x,z)=0$ for every x, since the intersection in (5.13) is empty.

Let us assume that $|z|\le\delta$. Observe that $S(x,z)$ counts the number of integers satisfying both (5.12) and (5.13); the former restriction implies that $S(x,z)\le(b-a)n-|m|$, where $m\in[-an,an]$, and the latter $S(x,z)\le n(\delta-|z|)$.

A detailed analysis of the situation gives us the following bounds for $S(x,z)$, when $m\in[-2an+\delta n/2,2an-\delta n/2]$ and $|z|\le\delta$:

- If $m\le 0$ then

$$S(x,z)=\begin{cases}(\delta-|z|)n+O(1) & \text{if } x\in\left[-a+\frac{\delta}{2},a+\frac{m}{n}-\frac{\delta}{2}\right]\\ O(\delta n) & \text{if } x\in\left[-a,-a+\frac{\delta}{2}\right]\cup\left[a+\frac{m}{n}-\frac{\delta}{2},a+\frac{m}{n}+\frac{\delta}{2}\right]\\ 0 & \text{if } x>a+\frac{m}{n}+\frac{\delta}{2}\end{cases}. \tag{5.14}$$

Thus, we have

$$\int S(x,z)dz=\begin{cases}\delta^2n+O(\delta) & \text{if } x\in\left[-a+\frac{\delta}{2},a+\frac{m}{n}-\frac{\delta}{2}\right],\\ 0 & \text{if } x>a+\frac{m}{n}+\frac{\delta}{2}\\ O(\delta^2n) & \text{otherwise.}\end{cases}$$

Since f is bounded, this gives:

$$\begin{aligned}J_1&=\frac{1}{\delta}\iint f(x)f\left(\tfrac{m}{n}-x\right)S(x,z)dxdz\\ &=(\delta n+O(1))\int_{-a+\frac{\delta}{2}}^{a+\frac{m}{n}-\frac{\delta}{2}}f(x)f\left(\tfrac{m}{n}-x\right)dx\\ &\quad+O(\delta n)\int_{-a}^{-a+\frac{\delta}{2}}f(x)f\left(\tfrac{m}{n}-x\right)dx+O(\delta n)\int_{a+\frac{m}{n}-\frac{\delta}{2}}^{a+\frac{m}{n}+\frac{\delta}{2}}f(x)f\left(\tfrac{m}{n}-x\right)dx\\ &=(\delta n+O(1))\left((f*f)\left(\tfrac{m}{n}\right)-\int_{-a}^{-a+\frac{\delta}{2}}f(x)f\left(\tfrac{m}{n}-x\right)dx-\int_{a+\frac{m}{n}-\frac{\delta}{2}}^{a}f(x)f\left(\tfrac{m}{n}-x\right)dx\right)\\ &\quad+O(\delta^2n)\\ &=(f*f)\left(\tfrac{m}{n}\right)\delta n+O(1)+O(\delta^2n).\end{aligned}$$

Let us recall that

$$\int_{a+\frac{m}{n}-\frac{\delta}{2}}^{a}f(x)f\left(\tfrac{m}{n}-x\right)dx=\int_{a+\frac{m}{n}-\frac{\delta}{2}}^{a+\frac{m}{n}}f(x)f\left(\tfrac{m}{n}-x\right)dx$$

since for any $x>a+\frac{m}{n}$ we have $f\left(\frac{m}{n}-x\right)=0$.

- If $m \geq 0$ then

$$S(x,z) = \begin{cases} (\delta - |z|)n + O(1) & \text{if } x \in \left[-a + \frac{m}{n} + \frac{\delta}{2}, a - \frac{\delta}{2}\right] \\ O(\delta n) & \text{if } x \in \left[-a + \frac{m}{n} - \frac{\delta}{2}, -a + \frac{m}{n} + \frac{\delta}{2}\right] \cup \left[a - \frac{\delta}{2}, a\right] \\ 0 & \text{if } x < -a + \frac{m}{n} - \frac{\delta}{2} \end{cases}.$$

and, analogously, we have $J_1 = (f * f)\left(\frac{m}{n}\right)\delta n + O(1) + O(\delta^2 n)$.

We now estimate J_2. Writing $\Delta(x,z) = f(x)\left(f\left(\frac{m}{n} - x + z\right) - f\left(\frac{m}{n} - x\right)\right)$, we observe that $|\Delta(x,z)| = O(\|f\|_\infty^2) = O(1)$, for every $x \in [-a,a]$ and $z \in [-\delta,\delta]$, and therefore for any interval I

$$\int_{-\delta}^{\delta}\int_I |\Delta(x,z)|dxdz \ll \delta|I|. \tag{5.15}$$

Also observe that

$$\left|\int \Delta(x,z)dx\right| = |(f*f)\left(\tfrac{m}{n}\right) - f*f\left(\tfrac{m}{n} + z\right)| \leq \epsilon(f,\delta), \tag{5.16}$$

where $\epsilon(f,\delta) = \max_{|u-v|\leq\delta}|(f*f)(u) - (f*f)(v)|$. Observe that since f is integrable and bounded in $[-a,a]$ then $f*f$ is continuous in $[-2a, 2a1]$ and we have that $\epsilon(f,\delta) = o(1)$, since $\delta = o(1)$.

From (5.14) and (5.15), we have for $-2an + \frac{\delta n}{2} \leq m \leq 0$

$$\begin{aligned} J_2 &= \delta^{-1}\iint \Delta(x,z)S(x,z)dxdz \\ &= \delta^{-1}\int_{-\delta}^{\delta}\int_{-a+\frac{\delta}{2}}^{a-\frac{\delta}{2}+\frac{m}{n}} \Delta(x,z)(\delta n - n|z|)dxdz + O(1) + O(\delta^2 n), \end{aligned}$$

where the $O(1)$ term comes from the $O(1)$ term in (5.14) and the fact that Δ is bounded and the $O(\delta^2 n)$ term comes from the integral with x in

$$\left[-a, -a + \frac{\delta}{2}\right] \cup \left[a + \frac{m}{n} - \frac{\delta}{2}, a + \frac{m}{n} - \frac{\delta}{2}\right],$$

using (5.15). Again, using (5.15),the integral can be extended to x in $[-a,a]$ adding only a factor $O(\delta^2 n)$. Thus

$$J_2 = \delta^{-1}\int_{-\delta}^{\delta}\int_{-a}^{a} \Delta(x,z)(\delta n - n|z|)dxdz + O(1) + O(\delta^2 n).$$

Using (5.16),

$$\begin{aligned} |J_2| &\leq n\int_{-\delta}^{\delta}\epsilon(h,\delta)dz + n\delta^{-1}\int_{-\delta}^{\delta}\epsilon(h,\delta)|z|dz + O(1) + O(\delta^2 n) \\ &= O\left(\delta n \epsilon(h,\delta)\right) + O(1) + O(\delta^2 n). \end{aligned}$$

These ideas can be applied to obtain the same upper bound for J_2 in the opposite range for m.

Observe that:

- If $m \leq \frac{\delta n}{2}$ and $x < \frac{m}{n}$ then

$$S(x,z) = O(1) + \begin{cases} 0 & \text{if } z \leq x - \frac{\delta}{2} - \frac{m}{n} \\ m - nx + \frac{\delta n}{2} + nz & \text{if } z \in [x - \frac{\delta}{2} - \frac{m}{n}, x - \frac{\delta}{2}] \\ m & \text{if } z \in [x - \frac{\delta}{2}, x + \frac{\delta}{2} - \frac{m}{n}] \\ nx + \frac{\delta n}{2} - nz & \text{if } z \in [x + \frac{\delta}{2} - \frac{m}{n}, x + \frac{\delta}{2}] \\ 0 & \text{if } z \geq x + \frac{\delta}{2} \end{cases},$$

so in this case

$$T(x) = \delta n m + O(\delta n)$$

and

$$J_1 = h\left(\frac{m}{n}\right)(nm + O(n)).$$

The same thing happens for $m > 2n - \frac{\delta n}{2}$. This means that we do not have the same order of magnitude for J_1 when m is very large or very small.

Putting all together we have that, for $m \in [-2an + \frac{\delta n}{2}, 2an - \frac{\delta n}{2}]$,

$$\mathbb{E}(X(m)) = \left((f * f)\left(\tfrac{m}{n}\right) + o(1)\right) n\delta. \tag{5.17}$$

We split these values of m into the two sets

$$M_0 = \left\{m \in \left[-2an + \tfrac{\delta n}{2}, 2an - \tfrac{\delta n}{2}\right] : \ \mathbb{E}(X(m)) < 2\epsilon_0 n\delta\right\}$$

and

$$M_1 = \left\{m \in \left[-2an + \tfrac{\delta n}{2}, 2an - \tfrac{\delta n}{2}\right] : \ \mathbb{E}(X(m)) \geq 2\epsilon_0 n\delta\right\},$$

where $\epsilon_0 = \min\left\{2, \frac{\epsilon}{10}, \frac{7\epsilon}{10\max_{x\in[-2a,2a]}(f*f)(x)}\right\}$.

Now we will use Chernoff's inequality, see Lemma 27, to see that $X(m)$ is close to its expectation in both sets. Observe that $X(m)$ is not a sum of independent Boolean variables but $X'(m) = X(m)/2$ is, so we can apply Chernoff's inequality to $X'(m)$.

We first prove that, for sufficiently large n, we have with probability at least 0.99 that $X(m) < 6\epsilon_0 n\delta$ for all $m \in M_0$. Since $\mathbb{E}(X'(m)) < \epsilon_0 n\delta$ for all $m \in M_0$, we can take $\gamma = \frac{3\epsilon_0 n\delta}{\mathbb{E}(X'(m))} - 1 > 2$ and, since $X'(m) \geq 0$ and using Chernoff's inequality,

$$\begin{aligned} \mathbb{P}(X'(m) > 3\epsilon_0 n\delta) &= \mathbb{P}\left(|X'(m) - \mathbb{E}(X'(m))| > \left(\tfrac{3\epsilon_0 n\delta}{\mathbb{E}(X'(m))} - 1\right)\mathbb{E}(X'(m))\right) \\ &\leq 2\exp\left(\tfrac{\mathbb{E}(X'(m))}{2} - \tfrac{3\epsilon_0 n\delta}{2}\right) \\ &\leq 2\exp\left(\tfrac{\epsilon_0 n\delta}{2} - \tfrac{3\epsilon_0 n\delta}{2}\right) \\ &\leq 2\exp\left(-\epsilon_0 n\delta\right). \end{aligned}$$

Then,

$$\begin{aligned} \mathbb{P}(X(m) > 6\epsilon_0 n\delta \text{ for some } m \in M_0) &= \mathbb{P}(X'(m) > 3\epsilon_0 n\delta \text{ for some } m \in M_0) \\ &\leq 4n\exp\left(-\epsilon_0 n\delta\right) \end{aligned}$$

which is less than 0.01 for sufficiently large n since $n\delta/\log n \to \infty$ when $n \to \infty$.

$$r_A(m) < 4e\epsilon n\delta$$

Consider the event $B_m := X(m) \geq 2K$. Using the union bound we have that

$$\begin{aligned}\mathbb{P}(B_m) &= \mathbb{P}\left(\sum_{i<m/2} X_i(m) \geq K\right) = \mathbb{P}\left(\cup_{\{i_1<\cdots<i_K\}\subseteq[\lceil m/2\rceil-1]}\left(X_{i_1}(m)=1\wedge\cdots\wedge X_{i_K}(m)=1\right)\right)\\ &\leq \sum_{i_1<\cdots<i_K<\frac{m}{2}} \mathbb{P}(X_{i_1}(m)=1)\cdots\mathbb{P}(X_{i_K}(m)=1).\end{aligned}$$

Then, for m in $M_0 = \{m : \mathbb{E}(X(m)) < 2\epsilon n\delta\}$,

$$\mathbb{P}(B_m) \leq \frac{\mathbb{E}^K(X(m)/2)}{K!} \leq \frac{(\epsilon n\delta)^K}{K!} \leq (e\epsilon n\delta/K)^K,$$

where in the last step we have used (remember Stirling's bounds) that $\frac{1}{K!} \leq \left(\frac{e}{K}\right)^K$ for every $K \in \mathbb{Z}_{\geq 0}$. We take $K = \lceil 2e\epsilon n\delta\rceil$ to get $\mathbb{P}(B_m) < 2^{-K}$. Thus

$$\mathbb{P}(B_m \text{ holds for some } m \in M_0) < n2^{-K+1} < 0.01$$

when n is large enough.

Now we prove that, for sufficiently large n, we have with probability at least 0.99 that $|X(m) - \mathbb{E}(X(m))| \leq \epsilon_0\mathbb{E}(X(m))$ for all $m \in M_1$.

For $m \in M_1$, using Chernoff's inequality ($\epsilon_0 \leq 2$) and since $E(X'(m)) \geq \epsilon_0 n\delta$,

$$\mathbb{P}(|X'(m) - \mathbb{E}(X'(m))| \geq \epsilon_0\mathbb{E}(X'(m))) \leq 2e^{-\epsilon_0^2\mathbb{E}(X'(m))/4} \leq 2e^{-\epsilon_0^3 n\delta/4}.$$

Now, $\mathbb{P}(|X(m) - \mathbb{E}(X(m))| \geq \epsilon_0\mathbb{E}(X(m))) = \mathbb{P}(|X'(m) - \mathbb{E}(X'(m))| \geq \epsilon_0\mathbb{E}(X'(m)))$, so

$$\mathbb{P}(|X(m) - \mathbb{E}(X(m))| \geq \epsilon_0\mathbb{E}(X(m)) \text{ for some } m \in M_1) \leq 4ne^{-\epsilon_0^3 n\delta/4}$$

which is less than 0.01 for sufficiently large n since $n\delta/\log n \to \infty$ when $n \to \infty$.

We consider a set A satisfying both conditions, $X(m) < 6\epsilon_0 n\delta$ for all $m \in M_0$ and $|X(m) - \mathbb{E}(X(m))| \leq \epsilon_0\mathbb{E}(X(m))$ for all $m \in M_1$. For sufficiently large n, since $r_A(m) \leq r_{A\hat{+}A}(m)+1 = X(m)+1$ and using (5.17), we have for $m \in M_0$

$$\left|\frac{r_A(m)}{n\delta} - (f*f)(m/n)\right| \leq \left|\frac{X(m)}{n\delta}\right| + \left|\frac{1}{n\delta}\right| + |(f*f)(m/n)| \leq 6\epsilon_0 + \epsilon_0 + (2\epsilon_0+\epsilon_0) \leq \epsilon$$

and for $m \in M_1$

$$\begin{aligned}\left|\frac{r_{A+A}(m)}{n\delta} - (f*f)(m/n)\right| &\leq \left|\frac{X(m)}{n\delta} - \frac{\mathbb{E}(X(m))}{n\delta}\right| + \left|\frac{\mathbb{E}(X(m))}{n\delta} - (f*f)(m/n)\right| + \left|\frac{1}{n\delta}\right|\\ &\leq \frac{\epsilon_0\mathbb{E}(X(m))}{n\delta} + \epsilon_0 + \epsilon_0 \leq \epsilon_0(f*f)(m/n) + 3\epsilon_0 \leq \epsilon.\end{aligned}$$

The expected value of $|A|$ is:

$$\mathbb{E}(|A|) = \sum_{i\in[-a,a]} \mathbb{P}(i \in A) = \sum_{i\in[-a,a]} \delta^{-1/2}\int_{I_i} f(x)dx = \delta^{-1/2}\int f(x)\sum_{i\in[-a,a]} I_i(x)dx.$$

We define $s(x) = \sum_{i\in[-a,a]} I_i(x)$ and, taking into account that $x \in I_i$ if and only if $nx - \frac{n\delta}{2} \leq i \leq nx + \frac{n\delta}{2}$,

$$s(x) = \begin{cases} \delta n + O(1) & \text{if } x \in [-\frac{1}{2} + \frac{\delta}{2}, \frac{1}{2} - \frac{\delta}{2}] \\ \frac{\delta n}{2} + n\left(\frac{1}{2} - x\right) + O(1) & \text{if } x \in [-\frac{1}{2}, -\frac{1}{2} + \frac{\delta}{2}] \\ \frac{\delta n}{2} + n\left(\frac{1}{2} + x\right) + O(1) & \text{if } x \in [\frac{1}{2} - \frac{\delta}{2}, \frac{1}{2}] \end{cases}.$$

$$s(x) = \begin{cases} 0 & \text{if } x \notin [-a, a], \\ \delta n + O(1) & \text{if } x \in [-a + \frac{\delta}{2}, a - \frac{\delta}{2}], \\ \frac{\delta n}{2} + n\left(\frac{1}{2} - |x|\right) + O(1) & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned} \mathbb{E}(|A|) =& \delta^{1/2} n \int_{-a+\delta/2}^{a-\delta/2} f(x)dx + \delta^{-1/2} O\left(\int_{-a+\delta/2}^{a-\delta/2} f(x)\right) + \frac{\delta^{1/2} n}{2} \int_{-a}^{-a+\delta/2} f(x)dx \\ &+ \delta^{-1/2} n \int_{-a}^{-a+\delta/2} \left(\tfrac{1}{2} + x\right) f(x)dx + \delta^{-1/2} O\left(\int_{-a}^{-a+\delta/2} f(x)dx\right) \\ &+ \frac{\delta^{1/2} n}{2} \int_{a-\delta/2}^{a} f(x)dx + \delta^{-1/2} n \int_{a-\delta/2}^{a} (a - x) f(x)dx \\ &+ \delta^{-1/2} O\left(\int_{a-\delta/2}^{a} f(x)dx\right) \\ =& \delta^{1/2} n \int_{-a}^{a} f(x)dx + O(\delta^{3/2} n) + O(\delta^{-1/2}) \\ =& \delta^{1/2} n \left(\int_{-a}^{a} f(x)dx + o(1)\right), \end{aligned}$$

where in the last equality we have used that $\delta = o(1)$ and $\frac{1}{\delta n} = o(1)$.

Now we use Chernoff's inequality (see Lemma 27) again to conclude that for every $\epsilon > 0$

$$\mathbb{P}\left(||A| - \mathbb{E}(|A|)| \geq \frac{\epsilon}{2}\mathbb{E}(|A|)\right) \leq 2e^{-\min\{\epsilon^2/16, \epsilon/4\}\delta^{1/2} n\left(\int f(x)dx + o(1)\right)}$$

which is less than or equal to 0.01 for sufficiently large n since $\delta^{1/2} n \to \infty$ when $n \to \infty$ (observe that we can suppose $\int f(x)dx > 0$ since if $\int f(x)dx = 0$ then $A = \emptyset$ trivially satisfies the conditions of the Theorem). So, with probability at least 0.99

$$\left|\frac{|A|}{n\delta^{1/2}} - \int f(x)dx\right| \leq \frac{\epsilon}{2} \int f(x)dx + (1 + \epsilon)o(1) \leq \epsilon \int f(x)dx.$$

□

As we defined in the first section, for a given real number $\alpha > 1/2$, if we consider the set $\mathcal{F}_\alpha$ of integrable nonnegative real bounded functions f with $\text{supp}(f) \subseteq [-\alpha/2, \alpha/2]$ such that $(f * f)(x) = \int f(t)f(x - t)dt \geq 1$ for every $x \in [-1/2, 1/2]$ then

$$\gamma(\alpha) = \inf_{f\in\mathcal{F}_\alpha} \int f(x)dx.$$

Corollary 17. *Let $\delta = \delta(n) > 0$ with $\delta(n) \to 0$ and $n\delta(n)/\log n \to \infty$ as $n \to \infty$. For every $\alpha > 1/2$, $f \in \mathcal{F}_\alpha$, $\epsilon > 0$ and $n > n_0(\epsilon, f)$ there exists a set of integers $A \subseteq [-\alpha n/2, \alpha n/2]$ such that*

$$|r_A(m) - n\delta| \le \epsilon n\delta \quad \text{for any } m \in \left[-\frac{n}{2}, \frac{n}{2}\right]$$

and satisfying

$$\left|\frac{|A|}{n\delta^{1/2}} - \int f(x)dx\right| \le \epsilon \int f(x)dx.$$

5.3.1 Combining interval sets with modular sets

A set $A \subseteq \mathbb{Z}$ is a $B[h_1, h_2]$-set modulo q if the representatives modulo q of the elements of A form a $B[h_1, h_2]$-set in $\mathbb{Z}_q$.

Lemma 14. *Let $A = \{a_1 < a_2 < \cdots < a_k\}$ be a subset of $\mathbb{Z}$, let $C \subseteq [0, q-1]$ be a $B[h_1, h_2]$-set modulo q and define*

$$B = (C + a_1 q) \cup \cdots \cup (C + a_k q).$$

Then, for any integer $m = ql + s$, with $0 \le s \le q-1$ and $l \in \mathbb{Z}$, we have that

$$h_1 r_A(l) - h_2|r_A(l) - r_A(l-1)| \le r_B(m) \le h_2 r_A(l) + h_2|r_A(l) - r_A(l-1)|$$

Proof. Given $m = ql + s$, $q \in \mathbb{Z}$ and $s \in [0, q-1]$ are uniquely determined. We consider the set $C_0 = \{(c, c') : c + c' = s\}$ and $C_1 = \{(c, c') : \ c + c' = s + q\}$. Then

$$\begin{aligned} r_B(m) &= r_A(l)|C_0| + r_A(l-1)|C_1| \\ &= r_A(l)(|C_0| + |C_1|) + (r_A(l-1) - r_A(l))|C_1| \end{aligned}$$

Using the triangle inequality and the fact that $h_1 \le |C_0| + |C_1| \le h_2$ we obtain the upper and lower bounds for $r_B(m)$. □

Theorem 26. *For every real number $\alpha > 1/2$,*

$$\limsup_{g\to\infty} \limsup_{n\to\infty} \frac{\gamma_g(\alpha, n)}{\sqrt{gn}} \le \gamma(\alpha).$$

Proof. First of all, we fix some $\delta(N)$ with $\delta(N) \to 0$ and $N\delta(N)/\log N \to \infty$ when $N \to \infty$, as in for Corollary 17. We have $\alpha > 1/2$, which is also fixed. For any sufficiently small $\epsilon > 0$, our plan is, for every sufficiently large g, to construct a sequence of g-basis $C_{g,n}$, for $n \ge n_0(g)$, with $\frac{|C_{g,n}|}{\sqrt{gn}} \le \gamma(\alpha)(1 + O(\epsilon))$.

Observe that the function $\gamma(\alpha)$ is a continuous decreasing function of α. Thus, for any given ϵ there exists $\alpha' < \alpha$ and a function $f \in \mathcal{F}_{\alpha'}$ with $\|f\|_1 \le \gamma(\alpha)(1 + \epsilon)$.

Now, since f is an integrable and bounded function, $(f * f)(x)$ is uniformly continuous and so for sufficiently large N we have

$$|(f*f)(x) - (f*f)(y)| \le \epsilon, \quad \text{for every } \ x, y \in [-1/2, 1/2] \ \text{ with } \ |x - y| \le \tfrac{1}{N}. \tag{5.18}$$

By Corollary 17, for sufficiently large N there is a set of integers $A \subseteq [-\alpha' N/2, \alpha' N/2]$ with

$$r_A(m) \geq N\delta(1-\epsilon) \text{ for every } m \in [-N/2, N/2] \tag{5.19}$$

and

$$|A| \leq N\delta^{1/2}(1+\epsilon)^2\gamma(\alpha). \tag{5.20}$$

Observe that the number of representations here depends on N.

We choose $N_0 = N_0(\delta, \alpha, \epsilon, f) \geq 1/\epsilon$ such that (5.18), (5.19), (5.20) and

$$\alpha' N < \alpha N - 2, \tag{5.21}$$

holds for every $N \geq N_0$.

Also, for every positive integer $s \geq 2$, by Corollary 15 (taking, for example, $k = s^2$), there exists r for which the sequence $q_0 = p_r^2 s$, $q_1 = p_{r+1}^2 s$, $q_2 = p_{r+2}^2 s$, ... (where p_i is the i-th prime) satisfies: for every $i = 0, 1, 2, \ldots$ there is a set $A_i \subseteq \mathbb{Z}_{q_i}$ with

$$s^5\left(1 - \tfrac{3}{s}\right) \leq r_{A_i}(m) \leq s^5\left(1 + \tfrac{9}{s}\right) \text{ for every } m \in \mathbb{Z}_{q_i}$$

and

$$|A_i| \leq (s^4 + s^2(p_{r+i} - 1) + 1)s \leq s^3(p_{r+i} + s^2). \tag{5.22}$$

Observe that the number of representations here does not depend on i, so we can construct larger and larger sets with the same bounds on the number of representations.

We choose $s = s(\epsilon) \geq 1/\epsilon$ and $r = r(s)$ according to Corollary 15.

Now, by the Prime Number Theorem

$$\frac{q_i - q_{i-1}}{q_i} = 1 - \left(\frac{p_{r+i-1}}{p_{r+i}}\right)^2 \to 0 \text{ when } i \to \infty$$

and, for reasons that will be clear later, we can choose i_1 such that

$$\alpha N(q_i - q_{i-1}) < q_i \quad \text{for every } i = i_1, i_1 + 1, \ldots, \tag{5.23}$$

we can choose i_2 such that

$$\frac{p_{r+i}}{p_{r+i-1}} + \frac{s^2}{p_{r+i-1}} \leq 1 + \epsilon \quad \text{for every } i = i_2, i_2 + 1, \ldots \tag{5.24}$$

and define $i_0 = \max\{i_1, i_2\}$.

Let us now consider the sequence of sets

$$B_i = ((A_i + a_1 q_i) \cup \cdots \cup (A_i + a_k q_i)) - \left\lfloor \frac{q_i}{2} \right\rfloor,$$

where $\{a_1 < a_2 \cdots < a_k\} = A$.

By Lemma 14, it follows that

$$r_{B_i}(m) \geq s^5\left(1 - \tfrac{3}{s}\right) r_A(l) - s^5\left(1 + \tfrac{9}{s}\right) |r_A(l) - r_A(l-1)|$$

for every $m = q_i l + t$ with $-\lfloor q_i/2 \rfloor \leq t \leq q_i - 1 - \lfloor q_i/2 \rfloor$ and every $l \in [-\alpha N/2, \alpha N/2]$. , where $h_1 = (16s^4 - 16s^3 - 8s^2)(s-1)$ and $h_2 = (16s^4 + 16s^3 + 24)(s+1)$.

Then, for any $N \geq N_0$, using Corollary 17 and the observation (5.18),

$$|r_A(l) - r_A(l-1)| \leq 3\epsilon N\delta$$

and from this and (5.19)

$$r_{B_i}(m) \geq N\delta s^5\left(1 - 4\epsilon - \tfrac{3}{s} - \tfrac{24\epsilon}{s}\right) \geq N\delta s^5\left(1 - 20\epsilon\right) = g_0(N)$$

for every $m \in [-Nq_i/2, Nq_i/2]$ because $s \geq 1/\epsilon$.

Observe that B_i is a $g_0(N)$-basis for $[-Nq_i/2, Nq_i/2]$ with

$$B_i \subseteq [-\alpha Nq_i/2 + q_i/2, -\alpha Nq_i/2 - q_i/2],$$

by (5.21), and that

$$|B_i| = |A_i||A| \leq N\delta^{1/2}(1+\epsilon)^2\gamma(\alpha)s^3(p_{r+i} + s^2),$$

by (5.20) and (5.22).

Now we are ready to recapitulate and complete the proof of the Theorem. For any given $g \geq g_0(N_0) = N_0\delta s^5\left(1 - 20\epsilon\right)$, there exists $N \geq N_0$ such that $g_0(N-1) < g \leq g_0(N)$.

For any given $n \geq Nq_{i_0} = n_0(g)$ there is i such that $Nq_{i-1} < n \leq Nq_i$ and we know how to construct B_i, a $g_0(N)$-basis for $[-Nq_i/2, Nq_i/2]$ with $B_i \subseteq [-\alpha Nq_i/2 + q_i/2, \alpha Nq_i/2 - q_i/2]$.

Now, B_i is obviously also a g-basis for $[-n/2, n/2]$, since $n \leq q_i N$ by definition and $g \leq g_0(N)$, and it follows from (5.23) that

$$\frac{\alpha Nq_i}{2} - \frac{q_i}{2} \leq \frac{\alpha Nq_{i-1}}{2} < \frac{\alpha n}{2},$$

which clearly implies that $B_i \subseteq [-\alpha n/2, \alpha n/2]$. Therefore, for every sufficiently large g and every $n \geq n_0(g)$ we constructed a g-basis for $[-n/2, n/2]$, namely $C_{g,n} := B_i$, supported in $[-\alpha n/2, \alpha n/2]$ and satisfying

$$\begin{aligned}
\frac{|C_{g,n}|}{\sqrt{gn}} &\leq \frac{|B_i|}{\sqrt{g_0(N-1)Nq_{i-1}}} \\
&\leq \gamma(\alpha)\,\frac{N\delta^{1/2}s^3(p_{r+i}+s^2)(1+\epsilon)^2}{\sqrt{N^2\delta s^6 p_{r+i-1}^2(1-20\epsilon)(1-\epsilon)}} \\
&\leq \gamma(\alpha)\left(\frac{p_{r+i}+s^2}{p_{r+i-1}}\right)\frac{(1+\epsilon)^2}{1-20\epsilon} \leq \gamma(\alpha)(1+O(\epsilon)),
\end{aligned}$$

where we have used (5.24) and $1/N \leq \epsilon$. This completes our proof. □

Corollary 16 and Theorem 26 prove:

Theorem 27. *For every real number $\alpha > 0$,*

$$\lim_{g\to\infty}\liminf_{n\to\infty}\frac{\gamma_g(\alpha,n)}{\sqrt{gn}} = \lim_{g\to\infty}\limsup_{n\to\infty}\frac{\gamma_g(\alpha,n)}{\sqrt{gn}} = \gamma(\alpha).$$

5.4 Taking the limit in α

Now we can prove our main result. Remember from the first section that $\gamma_g(n) = \min\{|A| : A \text{ is } g\text{-basis for } \{1,\dots,n\}\}$.

Theorem 20

$$\lim_{g\to\infty} \liminf_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}} = \lim_{g\to\infty} \limsup_{n\to\infty} \frac{\gamma_g(n)}{\sqrt{gn}} = \gamma.$$

Proof. We will prove

$$\lim_{g\to\infty} \liminf_{n\to\infty} \frac{\tilde{\gamma}_g(n)}{\sqrt{gn}} = \lim_{g\to\infty} \limsup_{n\to\infty} \frac{\tilde{\gamma}_g(n)}{\sqrt{gn}} = \gamma. \tag{5.25}$$

and, since $\lim_{\alpha\to\infty} \gamma_g(\alpha, n) = \tilde{\gamma}_g(n)$ where, for every fixed g, $\lim_{n\to\infty} \frac{\gamma_g(n)-\tilde{\gamma}_g(n)}{\sqrt{n}} = 0$, this will prove the theorem.

In order to prove (5.25), from Theorem 26 and Theorem 24, we have to show that

$$\lim_{\alpha\to\infty} \limsup_{g\to\infty} \limsup_{n\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \le \gamma \Rightarrow \limsup_{g\to\infty} \limsup_{n\to\infty} \lim_{\alpha\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \le \gamma. \tag{5.26}$$

and, for every fixed g,

$$\lim_{\alpha\to\infty} \liminf_{n\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \ge \gamma \Rightarrow \liminf_{n\to\infty} \lim_{\alpha\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \ge \gamma. \tag{5.27}$$

To prove (5.26) we just observe that, for every $\alpha \ge 1/2$, $\gamma_g(\alpha, n) \ge \lim_{\alpha\to\infty} \gamma_g(\alpha, n) = \tilde{\gamma}_g(n)$ since $\gamma_g(\alpha, n)$ is decreasing in α. Then

$$\gamma \ge \lim_{\alpha\to\infty} \limsup_{g\to\infty} \limsup_{n\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \ge \lim_{\alpha\to\infty} \limsup_{g\to\infty} \limsup_{n\to\infty} \frac{\tilde{\gamma}_g(n)}{\sqrt{gn}} = \limsup_{g\to\infty} \limsup_{n\to\infty} \frac{\tilde{\gamma}_g(n)}{\sqrt{gn}}.$$

To prove (5.27), we first remember that, from Theorem 24 for a fixed positive integer g and a fixed real $\epsilon > 0$, there exist $n_0(g, \epsilon)$ such that for every $\alpha > 1$ and for every $n \ge n_0(g, \epsilon)$

$$\frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \ge \gamma(\alpha) - \epsilon.$$

Then, for every fixed g and ϵ and for every $n \ge n_0(g, \epsilon)$

$$\lim_{\alpha\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \ge \gamma - \epsilon$$

and so,

$$\liminf_{n\to\infty} \lim_{\alpha\to\infty} \frac{\gamma_g(\alpha,n)}{\sqrt{gn}} \ge \gamma.$$

□

Appendices

Appendix A

Auxiliary results

A.1 Integer points on curves and varieties

In order to apply Theorem 1 to specific sets A, we need good estimates not only on the quantity $|\widehat{A}|$, but also on the cardinality of the set itself. In most of the applications the set A consists of the $\mathbb{F}_p$-points of certain algebraic variety. The following well known result will satisfy our needs.

Theorem 28 (Lang-Weil [66])**.** *Let V be an algebraic variety of dimension m, defined over the finite field $\mathbb{F}_q$ of q elements. The number of points of V in $\mathbb{F}_q$ is*

$$q^m + O\left(q^{m-1/2}\right).$$

The following results are essential to derive the estimates discussed in Chapter 2.

We will need the following result from Cilleruelo and Urroz [24] in the proof of Theorem 5.

Lemma 15. *Let $d \neq 0, 1$ be a fixed squarefree integer. On the conic, $x^2 - dy^2 = n$ an arc of length $n^{1/6}$ contains at most 2 lattice points.*

We will also require the following variant from Lemma 4 in [22].

Lemma 16. *Let $d \neq 0, 1$ be a fixed square-free integer. If $n = M^{O(1)}$, on the conic $x^2 - dy^2 = n$ an arc of length $M^{O(1)}$ contains, at most, $M^{o(1)}$ lattice points.*

Proof. This result is a variant of Lemma 4 in [22], where the conclusion was proved when $1 \leq x, y \leq M^{O(1)}$, (see Lemma 3.5 [98] for a more general result). If d is negative, the result is contained in Lemma 4 in [22] since it is clear that $1 \leq x, y \ll \sqrt{n} = M^{O(1)}$. We must study though the case where d is positive.

By symmetry we can consider only those arcs in the first quadrant, since any non-negative lattice point (x, y) will lead us to no more than four lattice points $(\pm x, \pm y)$. Let (u_0, v_0) be the minimal non-negative solution to the Pell's equation $x^2 - dy^2 = 1$, and $\xi = u_0 - \sqrt{d}v_0$ its

related fundamental unit in the ring of integers of $\mathbb{Q}\left(\sqrt{d}\right)$. Suppose that (x_0, y_0) is a positive solution to $x_0^2 - dy_0^2 = n$ that lies in our initial arc and let $t \in \mathbb{R}$ be the solution to

$$(x_0 + \sqrt{d}y_0)\xi^t = (x_0 - \sqrt{d}y_0)\xi^{-t}.$$

Then for $m = [t]$, we have $(x_0 + \sqrt{d}y_0)\xi^m = x_1 + \sqrt{d}y_1 \asymp \sqrt{n}$. This means that each solution in our initial arc corresponds to a 'primitive' solution lying in an arc of length $\ll \sqrt{n}$. Conversely, solutions in an arc of length $\ll \sqrt{n}$ can be taken to larger arcs by multiplying by powers of ξ^{-1}. Since our initial interval has length $M^{O(1)}$ there will be no more than $O(\log M)$ powers connected to each primitive solution. The term $O(\log M)$ is absorbed by $M^{o(1)}$.

On the other hand, we know by Lemma 4 in [22] that the number of lattice points in an arc of length $O(\sqrt{n})$ is $M^{o(1)}$. It follows that the number of solutions in the original arc will be bounded by $M^{o(1)}$. □

For more general curves, we need the following estimate of Bombieri and Pila [8] on the number of integral points on plane polynomial curves.

Lemma 17. *Let $\mathcal{C}$ be a plane absolutely irreducible curve of degree $d \geq 2$ and $H \geq \exp(d^6)$. Then the number of integral points on $\mathcal{C}$ and inside of a square $[0, H] \times [0, H]$ does not exceed $H^{1/d} \exp(12\sqrt{d \log H \log\log H})$.*

The following statement is a particular case of a more general result of Wooley [102, Theorem 1.1].

Lemma 18. *The number of solutions of the system of diophantine equations*

$$x_1^j + \ldots + x_8^j = x_9^j + \ldots + x_{16}^j, \quad j = 1, 2, 3$$

in integers x_i with $|x_i| \leq M$, $i = 1, \ldots, 16$, is at most $M^{10+o(1)}$.

Proof. Writing $x_i = X_i - M - 1$ with a positive integer $X_i \leq 2M + 1$, $i = 1, \ldots, 16$, after some trivial algebraic transformation we see that the number of solutions to the above equation is equal to $J_{8,3}(2M + 1)$, where $J_{k,m}(H)$ denotes the number of solutions of the system of m Diophantine equations in $2k$ integral variables $x_1, \ldots, x_{2k}$:

$$\begin{cases} x_1^m + \cdots + x_k^m &= x_{k+1}^m + \cdots + x_{2k}^m, \\ & \vdots \\ x_1 + \cdots + x_k &= x_{k+1} + \cdots + x_{2k}, \end{cases}$$
$$1 \leq x_1, \ \ldots, \ x_{2k} \leq H.$$

Since by the result of Wooley [102, Theorem 1.1] we have $\kappa(3) \leq 8$, the bound (2.32) applies with $H = 2M + 1$. □

We note that Lemma 18 can be formulated in a more general form with $\kappa(3)$ instead of 8 variables on each side, but this generalization (assuming possible improvements of the bound $\kappa(3) \leq 8$) does not affect our main results.

A.2 Uniform distribution and discrepancy of sequences

The following result is well-known and can be found, for example, in [77, Chapter 1, Theorem 1] (which is a more precise form of the celebrated Erdős–Turán inequality).

Lemma 19. *Let $\gamma_1, \dots, \gamma_M$ be a sequence of M points of the unit interval $[0,1]$. Then for any integer $K \geq 1$, and an interval $[\alpha, \beta] \subseteq [0,1]$, we have*

$$\#\{n \ : \ \gamma_n \in [\alpha,\beta]\} - M(\beta-\alpha) \ll \frac{M}{K} + \sum_{k=1}^{K} \left(\frac{1}{K} + \min\{\beta-\alpha, 1/k\}\right) \left|\sum_{n=1}^{M} \exp(2\pi i k \gamma_n)\right|.$$

To use Lemma 19 we also need an estimate on exponential sums with polynomials, which is essentially due to Weyl, see [62, Proposition 8.2].

Let $\|\xi\| = \min\{|\xi - k| \ : \ k \in \mathbb{Z}\}$ denote the distance between a real ξ and the closest integer.

Lemma 20. *Let $f(X) \in \mathbb{R}[X]$ be a polynomial of degree $m \geq 2$ with the leading coefficient $\vartheta \neq 0$. Then*

$$\left|\sum_{n=1}^{M} \exp(2\pi i f(n))\right| \ll M^{1-m/2^{m-1}} \left(\sum_{-M<\ell_1,\dots,\ell_{m-1}<M} \min\{M, \|\vartheta m! \ell_1 \dots \ell_{m-1}\|^{-1}\}\right)^{2^{1-m}}.$$

The result required to obtain the error term in Theorem 15 is the main theorem in [59], which deals with the distribution of fractional parts ν/p, where p is a prime less than or equal to n and ν is a root in $\mathbb{Z}/p\mathbb{Z}$ of a quadratic polynomial $f(x)$ with negative discriminant. For this f, we define the discrepancy $D_f(n)$ associated to the set of fractions $\{\nu/p : f(\nu) \equiv 0 \pmod p,\ p \leq n\}$ as

$$D_f(n) = \sup_{[u,v]\subseteq[0,1]} \left|(v-u) - \frac{1}{\pi(n)} \sum_{p\leq n} \sum_{\substack{u<\nu/p\leq v \\ f(\nu)\equiv 0 \pmod p}} 1\right|.$$

Under these assumptions, the result can be stated as follows:

Theorem 29 (Homma [59])**.** *Let f be any irreducible quadratic polynomial with integer coefficients and negative discriminant. Then for any $\epsilon < 8/9$ we have*

$$D_f(n) = O\left(\frac{1}{(\log n)^{\epsilon}}\right).$$

As a consequence of this result, we have the following lemma:

Lemma 21. *Let $g : [0,1] \to \mathbb{R}$ be any function of bounded variation, and $n < N$ two positive real numbers. Then for any $\epsilon < 8/9$*

$$\sum_{\substack{n<p<N \\ 0\le\nu<p \\ \nu^2\equiv -1\,(p)}} g\left(\frac{\nu}{p}\right) = 2\pi_1([n,N]) \int_0^1 g(t)\,\mathrm{d}t + O\left(\frac{N}{(\log N)^{1+\epsilon}}\right),$$

where $\pi_1(n) = |\{p : p \equiv 1 \pmod 4, p \le n\}|$.

Proof. We know by the Koksma–Hlawka identity (see Theorem 2.11 in [82]) that for any sequence $S = \{a_1, a_2, \dots, a_n\}$, $S \subset [0,1]$, with discrepancy $D_S(n)$ and for any $g : [0,1] \to \mathbb{R}$ with bounded variation, we have

$$\frac{1}{n}\sum_{i=1}^{n} g(a_i) = \int_0^1 g(t)\,\mathrm{d}t + O(D_S(n)),$$

so

$$\begin{aligned}\sum_{i=n}^{N} g(a_i) &= \sum_{i=1}^{N} g(a_i) - \sum_{i=1}^{n} g(a_i) \\ &= (N-n)\int_0^1 g(t)\,\mathrm{d}t + O(ND_S(N)) + O(nD_S(n)).\end{aligned}$$

In our case, using Theorem 29, we get

$$\sum_{\substack{n<p<N \\ 0\le\nu<p \\ \nu^2\equiv -1\,(p)}} g\left(\frac{\nu}{p}\right) = 2\pi_1([n,N]) \int_0^1 g(t)\,\mathrm{d}t + O\left(\frac{\pi_1(N)}{(\log N)^{\epsilon}}\right).$$

Using the rough estimate $\pi_1(N) = O\left(\frac{N}{\log N}\right)$ we get the required error term. □

A.3 Symmetric character sums

Let $\mathcal{X}$ be the set of all multiplicative characters modulo p and let $\mathcal{X}^* = \mathcal{X} \setminus \{\chi_0\}$ be the set of non principal characters.

We recall the Pólya-Vinogradov bound, see [62, Theorem 12.5].

Lemma 22. *For arbitrary integers W and Z, with $0 \le W < W + Z < p$, the bound*

$$\max_{\chi\in\mathcal{X}^*} \left|\sum_{z=W+1}^{W+Z} \chi(z)\right| \ll p^{1/2}\log p$$

holds.

We recall that Garaev and García [47], improving a result of Ayyad, Cochrane and Zheng [2] (see also [33]), have shown that for any integers W and Z

$$\sum_{\chi\in\mathcal{X}^*} \left|\sum_{z=W+1}^{W+Z} \chi(z)\right|^4 \ll pZ^2\left(\log p + \left(\log(Z^2/p)\right)^2\right). \tag{A.1}$$

Note that for any fixed $\varepsilon > 0$, if $Z \ge p^{\varepsilon}$ the right hand side of (A.1) is of the form $pZ^{2+o(1)}$. However for small values of Z, namely for $Z \ll (\log p)^{1/2}$, the bound (A.1) is trivial. We now combine (A.1) with a result of [22] to get the bound $pZ^{2+o(1)}$ for any Z.

Lemma 23. *For arbitrary integers W and Z, with $0 \le W < W + Z < p$, the bound*

$$\sum_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \ll pZ^{2+o(1)}$$

holds.

Proof. We can assume that $Z \le p^{1/4}$ since otherwise, as we have noticed before, the bound (A.1) implies the desired result. Now, using that for any integer z with $\gcd(z, p) = 1$, for the complex conjugated character $\overline{\chi}$ we have

$$\overline{\chi}(z) = \chi\left(z^{-1}\right),$$

we derive,

$$\sum_{\chi \in \mathcal{X}_0} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \le \sum_{\chi \in \mathcal{X}} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 = \sum_{z_1,z_2,z_3,z_4=W+1}^{W+Z} \sum_{\chi \in \mathcal{X}} \chi(z_1 z_2 z_3^{-1} z_4^{-1}).$$

Thus, using the orthogonality of characters we obtain

$$\sum_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \le pJ,$$

where J is number of solutions to the congruence

$$z_1 z_2 \equiv z_3 z_4 \pmod p, \qquad z_1, z_2, z_3, z_4 \in [W+1, W+Z].$$

By [22, Theorem 1], for any $\lambda \not\equiv 0 \pmod p$ the congruence

$$z_1 z_2 \equiv \lambda \pmod p, \qquad z_1, z_2 \in [W+1, W+Z]$$

has $Z^{o(1)}$ solutions, provided that $Z \le p^{1/4}$. Therefore $J \le Z^{2+o(1)}$ and the result follows. □

Consider, for given positive integers i, j, the number $T_{i,j}(B)$ of solutions to

$$r^i v^j \equiv u^i s^j \pmod p \tag{A.2}$$

with $(r, s), (u, v) \in B$. The following estimates were obtained for $T_{i,j}(B)$ in [28, 16].

Theorem 30. *For any prime p and any box $B = [R+1, M+1] \times [S+1, S+M]$, with $R, S \ge 1$, $M \ge 1$ and $R + M, S + M < p$, we have*

$$T_{i,j}(B) = d\frac{|B|^2}{p-1} + O\left(|B|^{1+o(1)}\right)$$

as $|B| \to \infty$, where $d = \gcd(i, j, p-1)$.

Proof. Using the orthogonality of characters, we write the the number of solutions to (A.2) with $(r,s),(u,v) \in B$ as

$$\begin{aligned} T_{i,j}(B) &= \sum_{r,u=R+1}^{R+M} \sum_{s,v=S+1}^{R+M} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \chi\left((r/u)^i (v/s)^j\right) \\ &= \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^2 \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2. \end{aligned}$$

The contribution to the above sum from d characters $\chi \in \mathcal{X}$ with $\chi^i = \chi^j = \chi_0$ is

$$dM^4/(p-1) = d|B|^2/(p-1).$$

Using Lemma 22, we see that the contribution to the above sum from at most i characters $\chi \in \mathcal{X}$ with $\chi^i = \chi_0$ and $\chi^j \neq \chi_0$ is bounded by

$$\frac{M^2}{p-1} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i = \chi_0}} \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2 \ll M^2 (\log p)^2,$$

when $M \geq p^{1/2}$, and bounded by

$$\frac{M^2}{p-1} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i = \chi_0}} \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2 \ll \frac{M^4}{p} (\log p)^2,$$

if $M < p^{1/2}$. In both cases, this quantity is $O\left(|B|^{1+o(1)}\right)$. The contribution from the characters $\chi \in \mathcal{X}$ with $\chi^j = \chi_0$ and $\chi^i \neq \chi_0$ can be estimated similarly as $O\left(|B|^{1+o(1)}\right)$.

Therefore

$$T_{i,j}(B) = d\frac{|B|^2}{p-1} + O\left(|B|^{1+o(1)} + W\right)$$

where

$$W = \frac{1}{(p-1)^2} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^2 \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2.$$

Using the Cauchy-Schwarz inequality, we derive

$$W^2 \leq \frac{1}{(p-1)^2} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^4. \tag{A.3}$$

When χ runs through $\mathcal{X}$ the power χ^h represents any other character in $\mathcal{X}$ no more that h times. Thus, by Lemma 23

$$\sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \ll \sum_{\chi \in \mathcal{X}^*} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \ll pM^{2+o(1)}$$

and similarly for the second double sums over s. This observation, combined with (A.3), implies that $W = O\left(|B|^{1+o(1)}\right)$, which concludes the proof. □

A.4 Pigeonhole principle

For an integer a we used $\|a\|_p$ to denote the smallest absolute value of a residue a modulo p, that is

$$\|a\|_p = \min_{k\in\mathbb{Z}} |a - kp|.$$

By the Dirichlet pigeonhole principle we easily obtain the following result.

Lemma 24. *For any real numbers $T_1, \dots, T_s$ with*

$$p > T_1, \dots, T_s \ge 1 \text{ and } T_1 \cdots T_s > p^{s-1}$$

and any integers $a_1, \dots, a_s$ there exists an integer t with $\gcd(t, p) = 1$ and such that

$$\|a_i t\|_p \ll T_i, \qquad i = 1, \dots, s.$$

A.5 Congruences with many solutions

The following result is used in the proofs of Theorems 8 and 13 in Chapter 2.

Lemma 25. *Let $f, g \in \mathbb{F}_p[X]$ be two polynomials of degrees n and m such that $m \nmid n$. Assume that the integers $x_1, \dots, x_n$ are pairwise distinct modulo p and $y_1, \dots, y_n$ are arbitrary integers. Then the congruence*

$$f(x) \equiv g(y) \pmod p, \qquad 0 \le x, y < p, \tag{A.4}$$

has at most mn solutions with

$$\det \begin{pmatrix} x^n & x^{n-1} & \dots & x & y \\ x_1^n & x_1^{n-1} & \dots & x_1 & y_1 \\ & & \dots & & \\ x_n^n & x_n^{n-1} & \dots & x_n & y_n \end{pmatrix} \equiv 0 \pmod p. \tag{A.5}$$

Proof. Since

$$\det \begin{pmatrix} x_1^n & x_1^{n-1} & \dots & x_1 \\ & & \dots & \\ x_n^n & x_n^{n-1} & \dots & x_n \end{pmatrix} = x_1 \dots x_n \prod_{1\le i<j\le n} (x_i - x_j) \not\equiv 0 \pmod p,$$

we deduce that, for any x and y, the last column in (A.5) is a unique modulo p linear combination of the previous columns. In particular, for every solution (x, y) to (A.4) and (A.5) we have $y \equiv h(x) \pmod p$ for some nontrivial polynomial $h(X) \in \mathbb{F}_p[X]$ that does not depend on x and y.

Now we insert this into (A.4). We observe that now the right hand side of (A.4), that is $g(h(x))$, is a nontrivial polynomial of degree $m \deg h$. Thus, the congruence (A.4) is a nontrivial polynomial congruence of degree d with $n \le d \le mn$. Therefore, it has at most mn solutions modulo p. □

A.6 Background on geometry of numbers

We recall that a lattice in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors. Let D be a symmetric convex body, that is, D is a compact convex subset of $\mathbb{R}^n$ with non-empty interior that is centrally symmetric with respect to 0. Then, for a lattice in $\Gamma \subseteq \mathbb{R}^n$ and $i = 1, \ldots, n$, the i-th successive minimum $\lambda_i(D, \Gamma)$ of the set D with respect to the lattice Γ is defined as the minimal number λ such that the set λD contains i linearly independent vectors of the lattice Γ. In particular $\lambda_1(D, \Gamma) \leq \ldots \leq \lambda_n(D, \Gamma)$. We recall the following result given in [5, Proposition 2.1] (see also [94, Exercise 3.5.6] for a simplified form that is still enough for our purposes).

Lemma 26. *We have,*

$$\#(D \cap \Gamma) \leq \prod_{i=1}^{n} \left(\frac{2i}{\lambda_i(D, \Gamma)} + 1 \right).$$

Using that

$$\frac{2i}{\lambda_i(D, \Gamma)} + 1 \leq (2i + 1) \max \left\{ \frac{1}{\lambda_i(D, \Gamma)}, 1 \right\}$$

and denoting, as usual, by $(2n+1)!!$ the product of all odd positive numbers up to $2n+1$, we derive:

Corollary 18. *We have,*

$$\prod_{i=1}^{n} \min\{\lambda_i(D, \Gamma), 1\} \leq (2n + 1)!!(\#(D \cap \Gamma))^{-1}.$$

A.7 The probabilistic method

The following well known result will be used in Chapters 3 and 5 (Corollary 1.9 in [94]).

Lemma 27 (Chernoff's inequality)**.** *Let $X = t_1 + t_2 + \cdots + t_n$, where the t_i are independent Boolean random variables. Then, for any $\gamma > 0$,*

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \gamma \mathbb{E}(X)) \leq 2e^{-\min\{\gamma^2/4, \gamma/2\}\mathbb{E}(X)}.$$

Observe that for $\gamma \leq 2$ the bound is $2e^{-(\gamma^2/4)\mathbb{E}(X)}$ and for $\gamma \geq 2$ the bound is $2e^{-(\gamma/2)\mathbb{E}(X)}$.

The second moment method is a very effective tool in Number Theory. Let X be a non-negative integral valued random variable and suppose we want to bound $\mathbb{P}(X = 0)$ given the value $\mu = \mathbb{E}(X)$. If $\mu < 1$ we may use the inequality $\mathbb{P}(X > 0) < \mathbb{E}(X)$ so that if $\mathbb{E}(X) \to 0$ then $X = 0$ almost always. Here we are imagining an infinite sequence of X dependent on some parameter n going to infinity.

Now suppose that $\mathbb{E}(X) \to \infty$. It does not necessarily follow that $X > 0$ almost always. Nevertheless, we can sometimes deduce $X > 0$ almost always if we have further information about $Var(X)$.

In Chapter 3 it is used in the version given by Corollary 4.3.3. of Alon, Spencer [1].

Theorem 31. *X be a non-negative integral valued random variable. If $\mathbb{E}(X) \to \infty$ and $Var(X) = o\left(\mathbb{E}(X)^2\right)$, as $n \to \infty$, then $X \sim \mathbb{E}(X)$ asymptotically almost surely. In particular, under these assumptions, $X > 0$ with probability tending to 1.*

Bibliography

[1] N. Alon and J. H. Spencer. *The Probabilistic Method*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., 2008.

[2] A. Ayyad, T. Cochrane, and Z. Zheng. The congruence $x_1x_2 \equiv x_3x_4 \pmod{p}$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums. *J. Number Theory*, 59(2):398–413, 1996.

[3] P. T. Bateman, J. Kalb, and A. Stenger. A limit involving least common multiples. *Amer. Math. Monthly*, 109:393–394, 2002.

[4] E. A. Bender and Z. Gao. Asymptotic enumeration of labelled graphs by genus. *Electron. J. Combin.*, 18(1):Paper 13, 28, 2011.

[5] U. Betke, M. Henk, and J. M. Wills. Successive-minima-type inequalities. *Discr. Comput. Geom.*, 9:165–175, 1993.

[6] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[7] E. Bombieri. On exponential sums in finite fields. *Amer. J. Math.*, 88:71–105, 1966.

[8] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.

[9] P. Borwein, S. Choi, and F. Chu. An old conjecture of Erdős-Turán on additive bases. *Math. Comp.*, 75(253):475–484, 2006.

[10] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski. On congruences with products of variables from short intervals and applications. *Proc. Steklov Math. Inst.*, 280:337–357, 2013.

[11] T. D. Browning. *Quantitative arithmetic of projective varieties*, volume 277 of *Progr. in Math.* Birkhäuser Verlag, Basel, 2009.

[12] E. R. Canfield, P. Erdős, and C. Pomerance. On a problem of Oppenheim concerning 'Factorisatio Numerorum'. *J. Number Theory*, 17:1–28, 1983.

[13] M.-C. Chang. Polynomial iteration in characteristic p. *J. Functional Analysis*, 263:3412–3421, 2012.

[14] M.-C. Chang. Expansions of quadratic maps in prime fields. *Proc. Amer. Math. Soc.*, 142:85–92, 2014.

[15] M.-C. Chang. Sparsity of the intersection of polynomial images of an interval. *Acta Arith.*, 165:243–249, 2014.

[16] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski, and A. Zumalacárregui. Points on curves in small boxes and applications. *Michigan Math. J.*, 63(3):503–534, 2014.

[17] G. Chapuy, É. Fusy, O. Giménez, B. Mohar, and M. Noy. Asymptotic enumeration and limit laws for graphs of fixed genus. *J. Combin. Theory Ser. A*, 118(3):748–777, 2011.

[18] P. L. Chebyshev. Memoire sur les nombres premiers. *J. de Math. Pures et Appl.*, 17(2):366–390, 1852.

[19] Y.-G. Chen. The analogue of Erdős-Turán conjecture in $\mathbb{Z}_m$. *J. Number Theory*, 128(9):2573–2581, 2008.

[20] J. Cilleruelo. The least common multiple of a quadratic sequence. *Compos. Math.*, 147(4):1129–1150, 2011.

[21] J. Cilleruelo. Combinatorial problems in finite fields and Sidon sets. *Combinatorica*, 32(5):497–511, 2012.

[22] J. Cilleruelo and M. Z. Garaev. Concentration of points on two and three dimensional modular hyperbolas and applications. *Geom. Funct. Anal.*, 21(4):892–904, 2011.

[23] J. Cilleruelo, M. Z. Garaev, A. Ostafe, and I. E. Shparlinski. On the concentration of points of polynomial maps and applications. *Math. Z.*, 272(3-4):825–837, 2012.

[24] J. Cilleruelo and J. Jiménez-Urroz. Divisors in a Dedekind domain. *Acta Arith.*, 85(3):229–233, 1998.

[25] J. Cilleruelo, F. Luca, J. Rué, and A. Zumalacárregui. On the sum of digits of some sequences of integers. *Cent. Eur. J. Math.*, 11(1):188–195, 2013.

[26] J. Cilleruelo, I. Ruzsa, and C. Vinuesa. Generalized Sidon sets. *Adv. Math.*, 225(5):2786–2807, 2010.

[27] J. Cilleruelo and I. Shparlinski. Concentration of points on curves in finite fields. *Monatsh. Math.*, 171(3-4):315–327, 2013.

[28] J. Cilleruelo, I. E. Shparlinski, and A. Zumalacárregui. Isomorphism classes of elliptic curves over a finite field in some thin families. *Math. Res. Lett.*, 19(2):335–343, 2012.

[29] J. Cilleruelo, C. Vinuesa, and A. Zumalacárregui. Representation functions in finite groups and bases for intervals. *preprint*, 2014.

[30] J. Cilleruelo, P. Šarka, J. Rué, and A. Zumalacárregui. The least common multiple of random sets of positive integers. *J. Number Theory*, 144:92–104, 2014.

[31] J. Cilleruelo and A. Zumalacárregui. An additive problem in finite fields with powers of elements of large multiplicative order. *Rev. Mat. Complut.*, 27(2):501–508, 2014.

[32] J. Cilleruelo and A. Zumalacárregui. Saving the logarithm factor in the error term estimates of some congruences problems. *preprint*, 2014.

[33] T. Cochrane and S. Shi. The congruence $x_1x_2 \equiv x_3x_4 \pmod m$ and mean values of character sums. *J. Number Theory*, 130(3):767–785, 2010.

[34] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[35] P. Deligne. *Cohomologie étale*. Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin-New York, 1977.

[36] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[37] G. A. Dirac. Note on a problem in additive number theory. *J. London Math. Soc.*, 26:312–313, 1951.

[38] W. Duke, J. B. Friedlander, and H. Iwaniec. Equidistribution of roots of a quadratic congruence to prime moduli. *Ann. of Math. (2)*, 141(2):423–441, 1995.

[39] P. Erdős and A. Rényi. Additive properties of random sequences of positive integers. *Acta Arith.*, 6:83–110, 1960.

[40] P. Erdős and A. Sárközy. Problems and results on additive properties of general sequences. II. *Acta Math. Hungar.*, 48(1-2):201–211, 1986.

[41] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt. Linear equations in variables which lie in a multiplicative group. *Ann. of Math. (2)*, 155(3):807–836, 2002.

[42] J. L. Fernández and P. Fernández. On the probability distrubution of the gcd and lcm of r-tuples of integers. *arXiv: 1305. 0536*, 2013.

[43] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.

[44] É. Fouvry. Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums. *Israel J. Math.*, 120:81–96, 2000.

[45] É. Fouvry and N. Katz. A general stratification theorem for exponential sums, and applications. *J. Reine Angew. Math.*, 540:115–166, 2001.

[46] M. Z. Garaev. On the logarithmic factor in error term estimates in certain additive congruence problems. *Acta Arith.*, 124(1):27–39, 2006.

[47] M. Z. Garaev and V. C. Garcia. The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications. *J. Number Theory*, 128(9):2520–2537, 2008.

[48] M. Z. Garaev and K.-L. Kueh. Distribution of special sequences modulo a large prime. *Int. J. Math. Math. Sci.*, (50):3189–3194, 2003.

[49] V. C. García. A note on an additive problem with powers of a primitive root. *Bol. Soc. Mat. Mexicana (3)*, 11(1):1–4, 2005.

[50] O. Giménez and M. Noy. Asymptotic enumeration and limit laws of planar graphs. *J. Amer. Math. Soc.*, 22(2):309–329, 2009.

[51] O. Giménez, M. Noy, and J. Rué. Graph classes with given 3-connected components: asymptotic enumeration and random graphs. *Random Structures Algorithms*, 42(4):438–479, 2013.

[52] G. Grekos, L. Haddad, C. Helou, and J. Pihko. On the Erdős-Turán conjecture. *J. Number Theory*, 102(2):339–352, 2003.

[53] C. S. Güntürk and M. B. Nathanson. A new upper bound for finite additive bases. *Acta Arith.*, 124(3):235–255, 2006.

[54] J. Gutiérrez and I. E. Shparlinski. Expansion of orbits of some dynamical systems over finite fields. *Bull. Aust. Math. Soc.*, 82:232–239, 2010.

[55] D. R. Heath-Brown. A mean value estimate for real character sums. *Acta Arith.*, 72:235–275, 1995.

[56] D. R. Heath-Brown. Arithmetic applications of Kloosterman sums. *Nieuw Arch. Wiskd.*, 5(1):380–384, 2000.

[57] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. of Math. (2)*, 155(2):553–595, 2002.

[58] D. R. Heath-Brown. *Equidistribution in number theory, An introduction*, chapter Analytic methods for the distribution of rational points on algebraic varieties, pages 139–168. Springer, Dordrecht, 2007.

[59] K. Homma. On the discrepancy of uniformly distributed roots of quadratic congruences. *J. Number Theory*, 128(3):500–508, 2008.

[60] S. Hong, G. Qian, and Q. Tan. The least common multiple of a sequence of products of linear polynomials. *Acta Math. Hungar.*, 135(1-2):160–167, 2012.

[61] C. Hooley. On exponential sums and certain of their applications. In *Number theory days, 1980 (Exeter, 1980)*, volume 56 of *London Math. Soc. Lecture Note Ser.*, pages 92–122. Cambridge Univ. Press, Cambridge-New York, 1982.

[62] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[63] A. Knopfmacher and F. Luca. Digit sums of binomial sums. *J. Number Theory*, 132(2):324–331, 2012.

[64] I. Konstantoulas. Lower bounds for a conjecture of Erdős and Turán. *Acta Arith.*, 159(4):301–313, 2013.

[65] S. V. Konyagin. Estimates for trigonometric sums over subgroups and for Gauss sums. In *IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001)*, pages 86–114. Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.

[66] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[67] H. W. Lenstra. Factoring integers with elliptic curves. *Ann. of Math.*, 126:649–673, 1987.

[68] F. Luca. Distinct digits in base b expansions of linear recurrence sequences. *Quaest. Math.*, 23(4):389–404, 2000.

[69] F. Luca. The number of nonzero digits of $n!$. *Canadian Math. Bull.*, 45:115–118, 2002.

[70] F. Luca. On the number of nonzero digits of the partition function. *Arch. Math. (Basel)*, 98(3):235–240, 2012.

[71] F. Luca and I. E. Shparlinski. On the g-ary expansions of Apéry, Motzkin, Schröder and other combinatorial numbers. *Ann. Comb.*, 14(4):507–524, 2010.

[72] F. Luca and I. E. Shparlinski. On the g-ary expansions of middle binomial coefficients and Catalan numbers. *Rocky Mountain J. Math.*, 41(4):1291–1301, 2011.

[73] W. Luo. Rational points on complete intersections over $\mathbb{F}_p$. *Internat. Math. Res. Notices*, 1999:901–907, 1999.

[74] O. Marmon. A generalization of the bombieri-pila determinant method. In *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, volume 377, pages 63–77, 2010.

[75] O. Marmon. he density of integral points on hypersurfaces of degree at least four. *Acta Arith.*, 141:211–240, 2010.

[76] M. Matolcsi and C. Vinuesa. Improved bounds on the supremum of autoconvolutions. *J. Math. Anal. Appl.*, 372(2):439–447.e2, 2010.

[77] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*. Amer. Math. Soc., Providence, 1994.

[78] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[79] P. Moree. Counting numbers in multiplicative sets: Landau versus Ramanujan. *Math. Newsl.*, 21(3):73–81, 2011.

[80] A. Mrose. Untere Schranken für die Reichweiten von Extremalbasen fester Ordnung. *Abh. Math. Sem. Univ. Hamburg*, 48:118–124, 1979.

[81] E. Nart. Counting hyperelliptic curves. *Adv. Math.*, 138:774–787, 2009.

[82] H. Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[83] A. Ostafe. Polynomial values in affine subspaces in finite fields. *preprint*, 2014.

[84] J. Pila. Density of integral and rational points on varieties. In *Columbia University Number Theory Seminar (New York, 1992)*, volume 228. Astérisque, 1995.

[85] J. Pila. Density of integer points on plane algebraic curves. *Inter. Math. Res. Notices*, 1996:903–912, 1996.

[86] O. Roche-Newton and I. E. Shparlinski. Polynomial values in subfields and affine subspaces of finite fieldspolynomial values in subfields and affine subspaces of finite fields. *preprint*, 2014.

[87] Z. Rudnick and A. Zaharescu. The distribution of spacings between small powers of a primitive root. *Israel J. Math.*, 120(part A):271–287, 2000.

[88] I. Z. Ruzsa. A just basis. *Monatsh. Math.*, 109(2):145–151, 1990.

[89] P. Salberger and T. D. Wooley. Rational points on complete intersections of higher degree, and mean values of weyl sums. *J. Lond. Math. Soc.*, 82:317–342, 2010.

[90] C. Sándor. A note on a conjecture of Erdős-Turán. *Integers*, 8:A30, 4, 2008.

[91] A. Schinzel and W. M. Schmidt. Comparison of L^1- and L^∞-norms of squares of polynomials. *Acta Arith.*, 104(3):283–296, 2002.

[92] I. E. Shparlinski. On the distribution of points on multidimensional modular hyperbolas. *Proc. Japan Acad. Ser. A Math. Sci.*, 83(2):5–9, 2007.

[93] C. L. Stewart. On the representation of an integer in two different bases. *J. Reine Angew. Math.*, 319:63–72, 1980.

[94] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010.

[95] Á. Tóth. Roots of quadratic congruences. *Internat. Math. Res. Notices*, 2014(12):719–739, 2000.

[96] Y. Tschinkel. Algebraic varieties with many rational points. In *Algebraic geometry*, volume 8 of *Clay Math. Proc.*, pages 243–334. Amer. Math. Soc., Providence, 2006.

[97] Vâjâitu and A. Zaharescu. Distribution of values of rational maps on the $\mathbb{F}_p$-points on an affine curve. *Monatsh. Math.*, 136:81–86, 2002.

[98] R. C. Vaughan and T. D. Wooley. Further improvements in Waring's problem. *Acta Math.*, 174(2):147–240, 1995.

[99] P. Šarka, J. Rué, and A. Zumalacárregui. On the error term of the logarithm of the lcm of a quadratic sequence. *J. Théor. Nombres Bordeaux*, 25(2):457–470, 2013.

[100] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.

[101] T. D. Wooley. Vinogradov's mean value theorem via efficient congruencing. *Ann. of Math.*, 175:1575–1627, 2012.

[102] T. D. Wooley. Vinogradov's mean value theorem via efficient congruencing, II. *Duke Math. J.*, 162:673–730, 2013.

[103] A. Zumalacárregui. Concentration of points on modular quadratic forms. *Int. J. Number Theory*, 7(7):1835–1839, 2011.